ソフトウェア管理に向けた
SBOM（Software Bill of Materials）の導入に関する
手引
ver 2.0

経済産業省　商務情報政策局
サイバーセキュリティ課

令和６年８月２９日

目次

1. 背景と目的 1

1.1. 背景 1
1.2. 目的 3
1.3. 主な対象読者 4
1.4. 主な対象ソフトウェア 4
1.5. 本書の構成と活用方法 5
1.6. 本手引のサマリー 6

2. SBOM の概要 9

2.1. SBOM とは 9
2.2. SBOM 導入のメリット 12
2.3. SBOM の「最小要素」 17
2.4. SBOM フォーマットの例 19
2.5. SBOM に関する誤解と事実 28

3. SBOM 導入に関する基本指針・全体像 32

3.1. SBOM 導入における基本指針 32
3.2. SBOM 導入プロセス 32

4. 環境構築・体制整備フェーズにおける実施事項・認識しておくべきポイント 34

4.1. SBOM 適用範囲の明確化 34
4.2. SBOM ツールの選定 38
4.3. SBOM ツールの導入・設定 43
4.4. SBOM ツールに関する学習 44

5. SBOM 作成・共有フェーズにおける実施事項・認識しておくべきポイント 46

5.1. コンポーネントの解析 46
5.2. SBOM の作成 50
5.3. SBOM の共有 51

6. SBOM 運用・管理フェーズにおける実施事項・認識しておくべきポイント 53

6.1. SBOM に基づく脆弱性管理、ライセンス管理等の実施 53
6.2. SBOM 情報の管理 55

7. 脆弱性管理プロセスの具体化 57

7.1. 目的 57
7.2. 脆弱性管理における課題・問題認識 57

7.3. プロセス全体像 58
7.4. 各フェーズの手順と方法 59

8. 付録：SBOM 対応モデル 83

8.1. 目的と背景 83
8.2. SBOM 可視化フレームワークと対応モデル 84
8.3. SBOM 対応モデルと活用方法 92
8.4. SBOM 対応モデルの参考例（自動車分野） 96
8.5. SBOM 対応モデルの参考例（ソフトウェア製品分野） 106
8.6. SBOM 対応モデルの参考例（医療機器分野） 115
8.7. SBOM 対応モデル（案）の分野横断比較 125

9. 付録：SBOM 取引モデル 127

9.1. 背景と目的（問題認識） 127
9.2. 概要 127
9.3. 取引モデルの考え方 128
9.4. SBOM 取引モデル 129
9.5. SBOM 対応モデルと SBOM 取引モデルの関係と位置づけ 132
9.6. 既存のモデル契約書との関係 133
9.7. 活用パターン 133
9.8. 課題と今後の検討の方向性 134

10. 付録：チェックリスト・用語集等 136

10.1. SBOM 導入に向けた実施事項チェックリスト 136
10.2. 用語集 139
10.3. 参考情報 143

1. 背景と目的

1.1. 背景

産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まる傾向にある。特に、近年は、産業機械や自動車等の制御にもソフトウェアの導入が進んでおり、IoT 機器・サービスや 5G 技術においても、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることで、様々な付加価値を創出していくことが期待されている。

企業等が利活用するソフトウェアに限らず、消費者が利活用するソフトウェアについても、安全・安心を担保するために、当該ソフトウェアの脆弱性を適切に管理することが求められる。企画・設計段階で脆弱性を含めないようソフトウェアが構成されていたとしても、製品出荷後に脆弱性が発見されることがあり、その場合、ソフトウェアを利活用する側でのソフトウェア更新等の対応が求められる。また、自社の製品・サービスで利活用しているソフトウェアの保守・サポートが終了する場合、それ以降に発見された脆弱性の管理について代替ソフトウェアへの変更を含めた検討が求められる。しかしながら、ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況がある。組織内の IT システムで利用されているソフトウェアを資産管理している組織は多いが、開発者が直接利用している上位のコンポーネントのみが資産管理の対象となり、直接利用のコンポーネントに内包されて間接的に利用される下位のコンポーネントの多くは資産管理の対象外となっている。したがって、脆弱性情報と資産管理台帳を照らし合わせるだけでは、下位のコンポーネントとして利用される OSS のようなコンポーネントにおいて脆弱性が発見された場合に、間接的な脆弱性の影響を検知することができない。

このようなソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一つの手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。SBOM とは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのことで、日本語では「ソフトウェア部品表」とも呼ばれる。SBOM は、米国商務省の電気通信情報局（NTIA）が 2018 年 7 月より開始した実証を通じて注目され始め、2021 年 5 月に米国バイデン大統領が署名した大統領令[1]を一つの起点として、世界的に普及が進みつつある。Linux Foundation が 2021 年の第 3 四半期にグローバルの 412 の組織を対象に実施した調査[2]

---

[1] Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] Linux Foundation, The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness
https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/
（日本語版） https://www.linuxfoundation.jp/blog/2022/05/the-state-of-software-bill-of-

では、調査対象の 48%の組織が SBOM を導入していることが明らかになったほか、Linux Foundation は、調査対象組織の SBOM 準備状況・計画状況を踏まえ 2022 年には 78%、2023 年には 88%の導入率になると推測している。

国内では、経済産業省において「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」（ソフトウェアタスクフォース）を 2019 年 9 月より開催し、SBOM も含めたソフトウェア管理手法等に関して幅広い議論を行ってきた。ソフトウェアタスクフォースの議論を通じ、SBOM 導入に向けて検討すべき課題として、SBOM 導入による費用対効果の課題、サプライチェーン上での SBOM 共有に関する課題、SBOM 管理に当たっての契約に関する課題、中小企業における SBOM 導入に関する課題等が提起された。このような課題を踏まえ、経済産業省は SBOM 導入に向けた実証を 2021 年以降に実施し、SBOM 導入にかかるコストや効果の評価を複数の産業分野で実施した。2021 年度の実証では自動運転システム開発向け検証基盤ソフトウェアを対象とし、2022 年度の実証では医療機器分野として歯科用 CT、自動車分野として自動車ヒーターコントローラー、ソフトウェア製品分野としてネットワーク脅威検知ソフト等を対象とした。これらの実証を通じて、以下に示すような SBOM のメリット・効果が確認でき、特にソフトウェアの脆弱性管理のメリットやライセンス管理のメリットがあり、その結果、開発生産性向上のメリットが得られることが分かった。

- 手作業でのコンポーネント管理の工数と SBOM を活用した管理の工数を比較した場合、SBOM を活用した管理の方が工数は小さくなる。SBOM を導入する際、初期工数は大きいものの、SBOM ツール[3]を活用することで負担は軽減される。
- SBOM を作成・管理することで、ソフトウェアに含まれているコンポーネントの脆弱性が発見された際の影響有無の特定までのリードタイムを短縮可能であり、脆弱性が残留するリスクの低減や脆弱性対応工数の低減につながる。特に、有償の SBOM ツールを活用することで、OSS 間の依存関係や OSS の再帰的な利用（再利用部品）も効率的に検出・管理できる。
- SBOM を作成・管理することで、ソフトウェアに含まれているコンポーネントのライセンス情報を確認でき、コンプライアンス上の過失を防ぐことができるため、ライセンス違反リスクの低減やライセンス管理工数の低減につながる。特に、SBOM ツールを活用することで、各ライセンスの内容表示や注意が必要なライセンスの警告等、コンプライアンス遵守のための機能が活用できるため、より効率的なライセンス管理が可能となる。

他方で、SBOM 導入に関して以下に示すような課題が明らかとなった。

- 対象とするソフトウェア・システムの全体構成が把握できていない場合、SBOM ツールの適用範囲を適切に設定できず、効果的なリスク管理が実施できない。
- SBOM ツールを導入するための環境整備や学習に工数を要する。

---

materials-sbom-and-cybersecurity-readiness/

[3] 本手引では、SBOM の作成、共有、活用、管理することができるツールを総称して「SBOM ツール」と呼ぶ。SBOM 管理ツール、OSS 管理ツール、ソフトウェア構成解析（SCA）ツール等と呼ばれることもある。

- 無償の SBOM ツールは、環境整備や学習に当たっての情報が不足しており、導入に大きな工数を要する。また、再帰的に利用される部品が十分に検出できない、取扱い可能な SBOM フォーマットに制限がある、ライセンスの検知漏れが発生する等、利用時に注意すべきことが多い。
- SBOM ツールを単に適用しただけでは、対象ソフトウェアに含まれるコンポーネントの検知漏れが発生する場合がある。
- SBOM ツールの出力結果について、コンポーネントの誤検出や検出漏れ、脆弱性情報の誤り等が発生する場合があるため、出力結果の精査が必要となる。
- サードパーティのコンポーネントについて、内部の構成や活用されている技術を把握できない状況で SBOM ツールの出力結果を精査することになるため、精査にかかる工数が大きくなる。
- 現状では、異なる SBOM ツールで生成した SBOM を読み込んで脆弱性管理に活用することができる SBOM ツールが少なく、異なる SBOM ツール間での SBOM の相互共有が困難である。
- 特定されたコンポーネントの脆弱性に対する対応要否・対応優先度の判断が困難である。
- SBOM を活用した脆弱性管理には、脆弱性特定、対応優先付けなどの課題があり具体的な対応法の情報が少ない。
- ソフトウェア開発委託や既製品の調達において、調達者と供給者の間で SBOM に関する要求や責任等を明確にするための契約事項についての情報が少ない。

総論として、SBOM を活用することで、効率的なソフトウェア管理を実施できることが確認できた一方で、実際の SBOM 導入に際しては様々な課題が存在することが明らかとなった。

1.2. 目的

本手引では、ソフトウェア管理に向けた SBOM の作成・共有・運用・管理に関する様々な課題の解決するために、SBOM の概要や SBOM 導入のメリット等、SBOM に関する基本的な情報を提供するとともに、ソフトウェアサプライヤーにおける SBOM 作成に向けた環境構築・体制整備、SBOM 作成・共有、そして SBOM の運用・管理に至る一連の SBOM 導入に向けたプロセスを示す。そして、企業における効率的・効果的な SBOM 導入を支援するために、各フェーズにおける主な実施事項や SBOM 導入に当たって認識しておくべきポイントを示す。さらに、SBOM の対応範囲の可視化の方法や契約書における要求事項についても示す。本手引は主にソフトウェアサプライヤーを対象としたものであるが、ソフトウェアを調達して利用する企業等においても、活用・参照することが可能である。なお、SBOM はソフトウェア管理の一手法であるため、SBOM を作成すること自体を目的とせず、SBOM を活用しつつ、適切なソフトウェア管理を目指すことが重要となる。近年のソフトウェア開発における OSS 活用増加の傾向を受け、ソフトウェアのセキュリティ対策に当たっては OSS の管理も重要となるが、OSS の管理に関するド

キュメントとして、経済産業省は「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」[4]を公開しているため、本手引と合わせて参照することが望まれる。

1.3. 主な対象読者

本手引では、ソフトウェアサプライヤーにおける開発・設計部門や製品セキュリティ担当部門（PSIRT 等）等のソフトウェアセキュリティに関わる部門と、経営層を主な対象としている。ソフトウェアセキュリティに関わる部門に対して、本手引では、ソフトウェア管理に向けた SBOM 導入の際に活用できる SBOM 導入に向けたプロセス、SBOM 導入に向けた主な実施事項及び SBOM 導入に当たって認識しておくべきポイントを記載している。また、ソフトウェア管理の一手法としての SBOM が、経営層に十分に認識されていないと考えられる場合には、「1.6 本手引のサマリー」を活用し、経営層と適切なコミュニケーションを行うことが期待される。経営層に対して、本手引では、SBOM 導入に関する意思決定を行う際に参照できる SBOM の効果・メリットや、SBOM に関する誤解と事実を示している。SBOM 導入に関する意思決定を行う際、「1.6 本手引のサマリー」の内容は認識しておくことが期待される。

「8 付録：SBOM 対応モデル」は、ソフトウェアや SBOM の供給者として、開発・運用部門やセキュリティ担当部門(PSIRT)を対象とし、ソフトウェアの調達者として、ユーザー企業、開発企業の調達部門、開発部門、品質保証部門、セキュリティ担当部門の担当者を対象とする。

「9 付録：SBOM 取引モデル」は、ソフトウェアの受発注者における SBOM に関する要求、責任、コスト負担等の規定を定める取引契約に係る法務担当者、開発者を主な想定読者とする。

いずれの内容も、ソフトウェアにおける脆弱性管理に課題を抱えている組織、SBOM という用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織、SBOM の必要性は理解しているが、導入に向けた取組内容が認識できていない組織等、主に SBOM 初級者に向けた内容となっている。関連して、本手引のライセンス管理に関する内容は、組織の法務・知財部門でも活用できるほか、全般的な内容は、ソフトウェアサプライヤーに限らず、ソフトウェアを調達して利用する企業においても一部活用可能である。SBOM の用途としては、脆弱性管理、ライセンス管理、輸出管理、特許管理など多様であるが、本書では、脆弱性管理、ライセンス管理に重点を置く。

1.4. 主な対象ソフトウェア

本手引では、主に単体で販売されるパッケージソフトウェアや機器に組込まれるソフトウェアを含むソフトウェア全般を対象とする。これらのソフトウェアに関する SBOM について、SBOM 導入に向けたプロセスを示すとともに、各プロセスにおける主な実施事項や SBOM 導入に当たって認識しておくべきポイントを

[4] 経済産業省、OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集
https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf

記載する。ハードウェアの脆弱性を含む部品管理も重要ではあるが、本書ではソフトウェアを対象とする。

1.5. 本書の構成と活用方法

SBOM を導入する組織は、本手引に基づき、SBOM に関する基本情報を認識するとともに、SBOM 導入に向けたプロセスを確認することが望まれる。そして、各ステップにおける主な実施事項及び SBOM 導入に当たって認識しておくべきポイントを確認しつつ、SBOM 導入を進めることが期待される。

2 章では、SBOM の基礎的な事項など概要をまとめている。3 章では、SBOM 導入の基本的な指針や導入プロセスの全体像をまとめている。4 章では、SBOM の初期導入に関する実施事項をまとめている。5 章、6 章では、初期導入後のプロジェクトごとの SBOM 作成・共有フェーズ及び運用・管理フェーズにおける実施事項等をまとめている。SBOM を用いた脆弱性特定や優先付けにおいては現状の脆弱性 DB 環境の課題があるため、7 章に示す解決策やノウハウを参考に、自組織に合った方法を選択・カスタマイズすることが期待される。SBOM の対応範囲を可視化し管理レベルを示す枠組みとして付録 8 が活用できる。取引者間の要求・責任を契約により明確に規定するためには付録 9 を参考とすることができる。なお、付録の 10.1 では、SBOM 導入の各ステップにおける実施事項をチェックリストとしてまとめているため、SBOM 導入に向けた取組時にあわせて参照することが望まれる。

1.6. 本手引のサマリー

《本手引のポイント》

- 企業経営へ影響を及ぼしうるソフトウェアのセキュリティ脅威が近年急激に増大している
- 脅威に対し、ソフトウェア管理の一手法である Software Bill of Materials（SBOM：エスボム）が注目を集めており、導入企業が世界的に増加している
- SBOM の活用により、ソフトウェアの脆弱性やライセンスの管理のリスク及びコストを低減可能である
- 本手引を活用し、ソフトウェア管理に向けた SBOM 導入の取組を進めることが期待される

《本手引の背景・概要》

【ソフトウェアサプライチェーンの脅威】

✓ ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアに対するセキュリティ脅威が近年急激に増大している。2021 年 12 月に発見された Apache Log4j の脆弱性は世界中に影響を及ぼしたほか、2019 年から 2022 年にかけてのソフトウェアサプライチェーン攻撃の年平均増加率が 742%に達したというデータもある。

✓ ソフトウェアに対するセキュリティ脅威は企業経営へ大きな影響を及ぼす。例えば、SolarWinds のサイバー攻撃の影響を受けた企業は、平均して年間収益額の約 11%の損害を被ったというデータもあるほか、製品に脆弱性が残存することで製品回収や販売停止につながった事例もある。

✓ ソフトウェアに対する脅威の状況に対し、ソフトウェアに含まれる脆弱性を適切に管理し、脆弱性が明らかになった際に迅速に対応するといったソフトウェア管理を効率的・効果的に実施していくことが重要である。

【ソフトウェア管理における SBOM 活用のメリット】

✓ このようなサプライチェーンを通じて開発されるソフトウェアの管理を効率化するための手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。SBOM とは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのことで、世界的に導入企業が増加しているほか、医療機器分野等の一部の分野では SBOM の推奨がされる等、規制や制度化も検討され始めている。

✓ 情報量が膨大となるソフトウェア管理に対し、機械処理可能な SBOM を導入することで、ソフトウェア管理に要する対応コストや人的コストを低減することができ、これにより開発生産性向上につながる。事実、経済産業省が実施した医療機器分野を対象とした実証では、SBOM を活用した脆弱性管理を行うことで、手動での管理と比較して、管理工数が 70%程度低減した。

✓ また、脆弱性管理上のメリットとして、SBOM を作成し、継続的に管理することで、ソフトウェアの透明性を高め、脆弱性残留リスクの低減が期待される。

✓ このようなことから、サプライチェーンを通じて SBOM を導入し、開発・運用に関わる企業組織がそれぞれ部品管理・脆弱性対応を効果的に分担することで、ベンダーへの負担を解消し、全体の効率

化を図ることが期待される。

- ✓ さらに、ライセンス管理上のメリットとして、SBOM を導入し、OSS のライセンス情報を管理することで、ライセンス違反リスクの低減にも寄与する。

【本手引の活用ポイント】

- ✓ 本手引では、SBOM に関する基本的な情報を提供するとともに、企業の効率的・効果的な SBOM 導入を支援するために、SBOM 導入に向けた主な実施事項及び SBOM 導入に当たって認識しておくべきポイントを示す。
- ✓ 効率的・効果的なソフトウェア管理に向け、本手引を活用し、経営層においては、SBOM 導入に関する意思決定を行うとともに、ソフトウェアセキュリティに関わる部門においては、SBOM 導入に向けた具体的な取組を進めることが期待される。

コラム：ソフトウェアのセキュリティ脅威に関する重要指数

ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアに対するセキュリティ脅威が近年拡大している。以下では、近年のソフトウェアのセキュリティ脅威に関する現状を示す重要な数値について紹介する。

***84%*：脆弱性が含まれるコードベースの割合**

2023 年に Synopsys 社が発表した 1,700 のコードベースを対象とした調査結果によれば、OSS を含むコードベースの割合は 96%であった。そのうち、84%のコードベースに少なくとも一つの脆弱性が含まれていた[5]。

***62%*：2021 年にソフトウェアサプライチェーン攻撃を受けた企業の割合**

2022 年に Anchore 社が発表した北米・EU・英国の企業 428 社を対象とした調査結果によれば、過去 1 年間でソフトウェアサプライチェーン攻撃の影響を受けた企業は 62%であった[6]。

***+742%*：2019 年から 2022 年にかけてのソフトウェアサプライチェーン攻撃の年平均増加率**

2023 年に Sonatype 社が発表した調査結果によれば、2019 年から 2022 年の 3 年間でのソフトウェアサプライチェーン攻撃の年平均増加率は 742%であり、2022 年には 88,000 件を超えた。2015 年 2 月～2019 年 6 月までの攻撃件数は 216 件であり、近年、ソフトウェアサプライチェーン攻撃の件数が指数関数的に増加している[7]。

***-11%*：SolarWinds のサイバー攻撃による企業収益額への影響（損害）**

2021 年に IronNet 社が発表した米国・英国・シンガポールの企業 473 社を対象とした調査結果によれば、85%の企業が SolarWinds のサイバー攻撃の影響を受けた、それら企業は、平均して年間収益額の約 11%の損害を被った[8]。

---

[5] Synopsys, 2023 Open Source Security and Risk Analysis Report
https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

[6] Anchore, 2022 Security Trends: Software Supply Chain Survey
https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/

[7] Sonatype, 8th Annual State of the Software Supply Chain Report
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

[8] IronNet, 2021 Cybersecurity Impact Report
https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf

2. SBOM の概要

2.1. SBOM とは

SBOM とは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストである。SBOM には、ソフトウェアに含まれるコンポーネントの名称やバージョン情報、コンポーネントの開発者等の情報が含まれ、OSS だけではなくプロプライエタリソフトウェアに関する情報も含めることができる。また、SBOM をソフトウェアサプライチェーンの上流から下流に向かって組織を越えて相互共有することで、ソフトウェアサプライチェーンの透明性を高めることが期待されており、特に、コンポーネントの脆弱性管理の課題に対する一つの解決策として期待されている。

SBOM のイメージをより具体化するために、以下のような簡易的なシナリオを考える。

- A 社は、B 社の Browser とコミュニティ P の Protocol という 2 つのコンポーネントを使用して、Application というソフトウェアを開発した。
- B 社の Browser は、C 氏が開発した Compression Engine のコンポーネントを使用している。
- B 社は、Browser に関する SBOM を自社で作成し、A 社に共有した。ただし、C 氏やコミュニティ P のコンポーネントに関する SBOM 情報を取得できなかったため、A 社にて、C 氏とコミュニティ P のコンポーネントの SBOM を作成した。

このシナリオにおけるプレイヤーやコンポーネントの関係性は図 2-1 のように表現できる。この図に示すとおり、多くの SBOM のエンティティは、ソフトウェアのサプライヤーの役割だけでなく、他者から共有された SBOM を利用する役割も担う。すなわち、別のエンティティから入手した SBOM の情報を活用するだけでなく、新たに開発したコンポーネントに関連する SBOM を作成し、その他のエンティティに SBOM を共有する役割も担うことがある。なお、ソフトウェアコンポーネントに関するサプライヤーと SBOM 作成者は一致することが理想的であるが、SBOM が完全に普及していない現状では必ずしも一致しない。今回のシナリオでは、B 社は自社内で SBOM を作成しているため、Browser のコンポーネントに関するサプライヤーと SBOM 作成者は一致しているが、Protocol の場合、コミュニティ P では SBOM 作成を行わず A 社にて SBOM 作成を行ったため、サプライヤーはコミュニティ P となるが、SBOM 作成者は A 社となる。

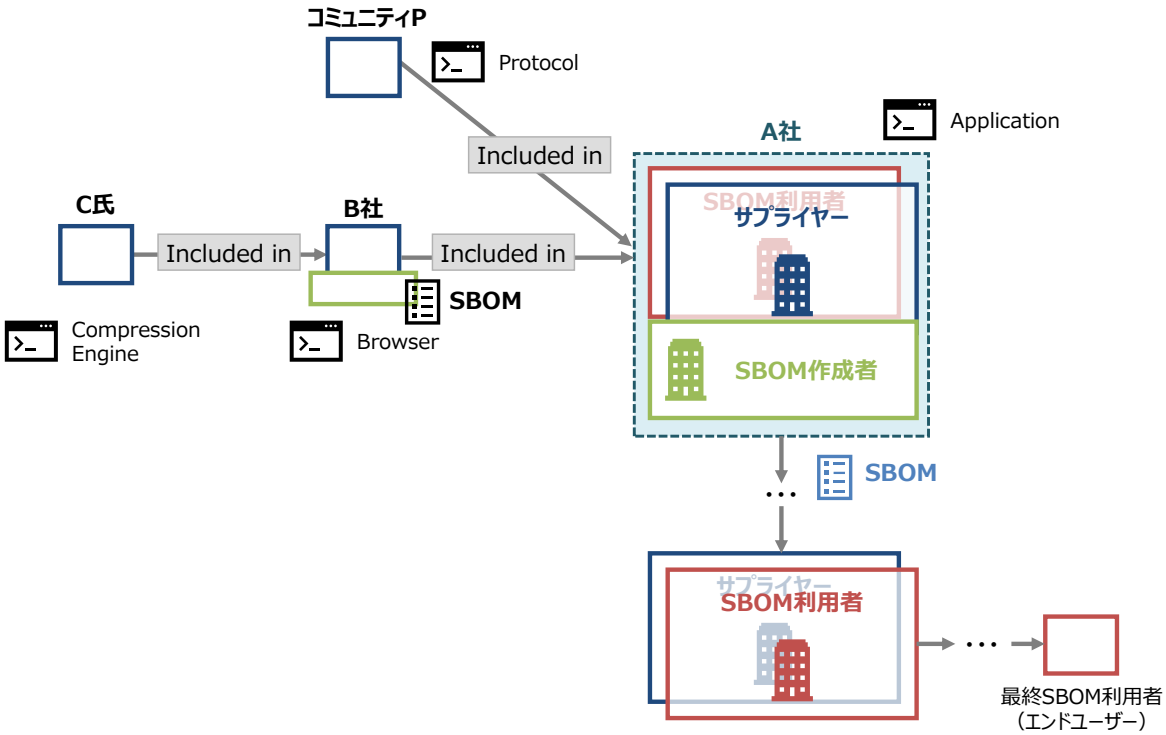

図 2-1 簡易シナリオにおけるプレイヤー間の関係性

上記のシナリオにおいて、A 社が作成する SBOM の概念的イメージは表 2-1 のように与えられる。このイメージでは、各コンポーネントについて、そのサプライヤーやバージョン、コンポーネント間の依存関係、SBOM 作成者等が一覧化されている。SBOM を作成することで、各コンポーネントがいつ、誰によって開発され、他のコンポーネントとどのような依存関係があり、当該コンポーネントに関する SBOM が誰によって作成されたかを特定・管理することが可能となる。これにより、特定のコンポーネントの脆弱性が明らかになったとき、その脆弱性の影響を受けるコンポーネントが含まれているかを即座に認識することができ、脆弱性に対する迅速な対応を行うことができる。そして、SBOM が組織を越えて相互共有されることで、各コンポーネントに関する情報が可視化されることとなり、ソフトウェアサプライチェーンの透明性向上に寄与することとなる。

表 2-1 簡易シナリオにおける SBOM の概念的イメージ

#	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM 作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in Application	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in Browser	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in Application	Company A	05-09-2022 13:00:00

上記の簡易シナリオに基づく表 2-1 の SBOM はあくまでイメージであり、このレベルの記載内容であれば、あえて SBOM として管理する必要はないかもしれない。しかしながら、実際のソフトウェアは、図 2-1 で描かれるようなシンプルなサプライチェーン構造ではなく、複雑な構造の下で開発される。また、自社で開発したプロプライエタリソフトウェアだけでなく、他社が開発したコンポーネントも含まれ、それぞれが複雑な依存関係を持つこととなる。したがって、ソフトウェアのリスク管理やソフトウェアサプライチェーンの透明性を高めるために、SBOM を用いて、ソフトウェアに含まれるコンポーネントの情報をその依存関係も含めて管理することが重要となる。

コラム：SBOM と食品表示とのアナロジー

SBOM は、食品の包装に記載されている食品表示に類似している。食品に含まれる原材料を可視化した食品表示を見ることで、アレルギー事故等による健康危害防止や食の禁忌への対応が可能となる。マカロニサラダを例として考えたとき、食品サプライチェーンを通じた製造・加工等の結果、各原材料を含んだ図 2-2 に示すような食品表示が作成される。SBOM は、食品表示のようにソフトウェアに含まれるコンポーネントの情報を示したリストであり、これらの情報が可視化されることで、脆弱性への対応やリスク管理が容易となる。食品表示が食品サプライチェーンの透明性向上に寄与していることと同様に、SBOM もソフトウェアサプライチェーンの透明性向上に寄与するものである。ただし、食品表示と異なり、SBOM はコンポーネント名だけでなく、そのバージョンや依存関係についても記載するため、食品表示より複雑なリストとなることに留意したい。また、多くの SBOM は作成後も動的に変更されるため、SBOM 利用者での管理が重要となることに留意したい。

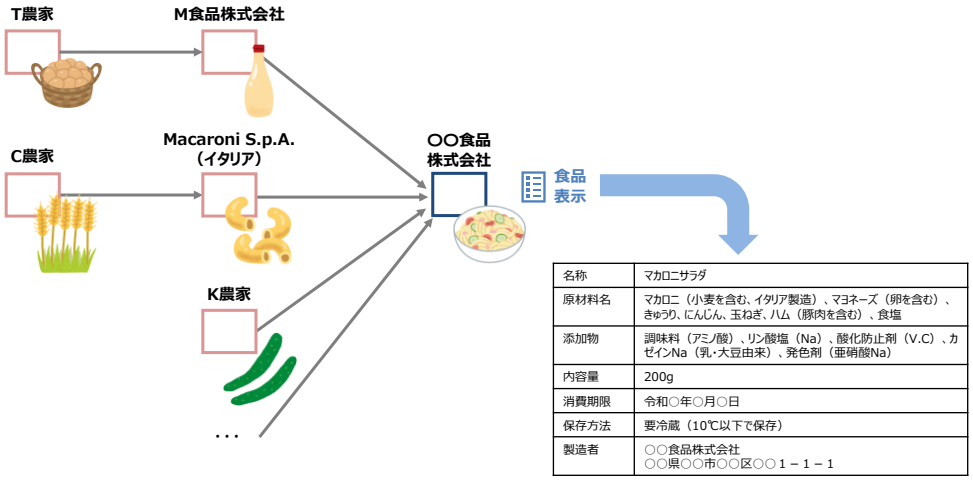

図 2-2 食品サプライチェーン及び食品表示の概念的イメージ

2.2. SBOM 導入のメリット

SBOM 導入による代表的なメリットとして、表 2-2 に示すとおり、脆弱性管理のメリット、ライセンス管理のメリット、そして、開発生産性向上のメリットの 3 つが挙げられる。それぞれのメリットにおいて、SBOM 導入組織に対する脆弱性管理・ライセンス管理・開発生産性向上の直接的なメリットのほか、製品価値や企業価値等に対する間接的なメリットも存在する。

表 2-2 SBOM 導入の主なメリット

メリット区分		メリット項目	主な内容
脆弱性管理のメリット	直接的メリット	脆弱性残留リスクの低減	脆弱性に関する情報を収集し、SBOM の情報と突合して脆弱性を検出することで、ソフトウェアにおいて脆弱性が残留するリスクを低減できる。
		脆弱性対応期間の短縮	SBOM ツール等を用いることにより新たな脆弱性をリアルタイムで検出し、影響を判断することで、初動期間を短縮できる。
		脆弱性管理にかかるコストの低減	SBOM ツールを用いた自動管理により、手動での管理と比較して、管理コストを低減できる。
	間接的メリット	製品価値・企業価値向上	製品に含まれる脆弱性の低減や脆弱性対応の迅速化により、製品や企業の価値が向上する。
		サイバー衛生の向上（Cyber Hygiene）	脆弱性の少ない製品が増えることで、サイバー空間全体のセキュリティが向上する。（踏み台悪用により攻撃を受けるリスクが低減できる。ソフトウェアの取引者以外にもメリットが得られるなどの外部経済効果が高まる）
ライセンス管理のメリット	直接的メリット	ライセンス違反リスクの低減	OSS の特定漏れによるライセンス違反のリスクを低減できる。
		ライセンス管理にかかるコストの低減	SBOM ツールを用いた自動管理により、手動での管理と比較して、管理コストを低減できる。
	間接的メリット	製品価値・企業価値向上	製品のライセンス違反リスクの低減により、製品や企業の価値が向上する。
開発生産性向上のメリッ	直接的メリット	開発遅延の防止	コンポーネントに関する問題を早期に特定することで、開発遅延の発生を防ぐことができ

メリット区分		メリット項目	主な内容
ト			る。
		開発にかかるコストの低減	コンポーネントに関する問題を早期に特定することで、対応コストを低減できる。
		開発期間の短縮	使用するコンポーネントを選定する際、類似製品に関する過去の SBOM を参照することで、選定に関する工数を削減できる。
		コンプライアンス対応の効率化	認証対応、法令対応、輸出規制管理対応などの効率化
		現場のモチベーション改善	業務の効率化、生産性向上の結果、現場のモチベーションの改善につながる。

SBOM 導入のメリットのうち、最も注目されているのが脆弱性管理のメリット、すなわち、ソフトウェアにおける脆弱性を検出し、優先度付けを行った上で修正及び軽減するといった一連の脆弱性対応プロセスにおけるメリットである。近年のソフトウェアの多くは複雑なサプライチェーン構造の下で開発され、自社で開発したプロプライエタリソフトウェアだけでなく、他社や OSS コミュニティが開発したコンポーネントも多く含む。そして、これらのコンポーネントが複雑な階層構造や依存関係を持つことが多い。例えば、ある Java アプリケーションが Apache Log4j をコンポーネントとして用いている場合、Log4j は下位のコンポーネントに位置づけられ、通常のコンポーネント管理では特定が難しい場合がある。しかしながら、下位のコンポーネントであっても、当該コンポーネントが脆弱性を含んでいた場合にセキュリティ上の影響を受ける可能性がある。

脆弱性残留リスクの低減のために、利用しているコンポーネントに関する情報に基づき、脆弱性の継続的な監視を有効に実施することが重要となる。この点、SBOM を導入し、各コンポーネントについて脆弱性データベースとの突合を行うことで、既知の脆弱性の影響を受けないかを効率的に確認することができ、結果として、ソフトウェアにおいて脆弱性が残留するリスクを低減できる。また、あるコンポーネントについて新たな脆弱性が明らかになったとき、SBOM を用いた管理を行っていない場合、自社のソフトウェアがそのコンポーネントを含んでいるか否かも分からず、知らぬ間に脆弱性の影響を受ける可能性もある。図 2-3 に示すとおり、SBOM を導入していれば、あるコンポーネントにおいて脆弱性が明らかになった場合に、その脆弱性の影響を即座に認識することができ、脆弱性対応にかかる期間を短縮することができる。加えて、パートナー企業、脆弱性の影響を受ける組織、ソフトウェア利用者等とソフトウェアに関する情報を組織間で共有することで、脆弱性対応にかかる期間を短縮できるほか、サプライチェーン上で第三者によりコンポーネントの書換えや不正な追加が行われた場合にも、その実態把握に資するものとなる。また、組織間共有に当たって SBOM を活用することで、ソフトウェア情報に関する共有に要する工数を低減することができる。

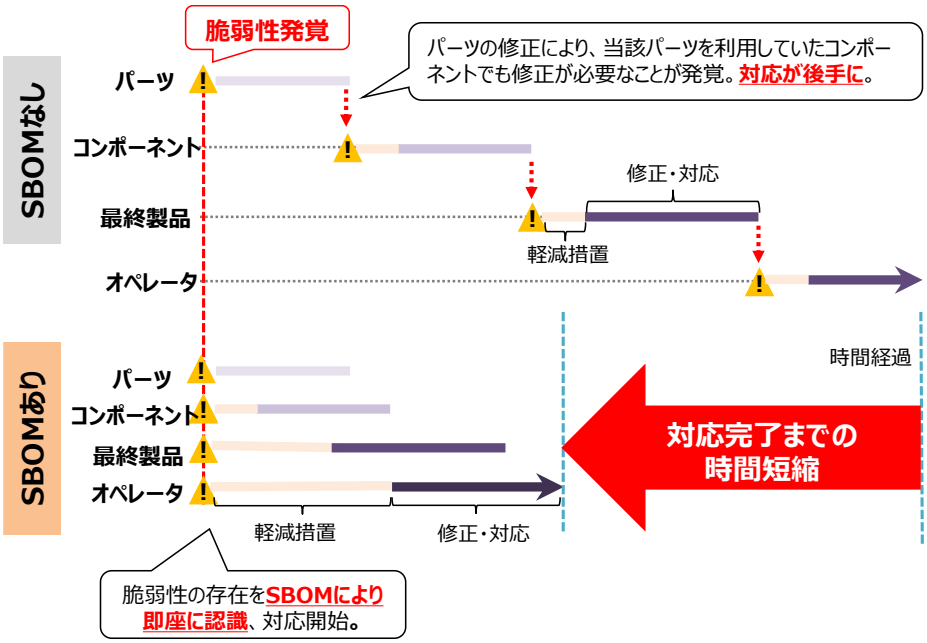

図 2-3 SBOM 導入による脆弱性対応期間短縮のメリット

そして、SBOM を導入することで、脆弱性管理にかかるコストを低減することができる。2022 年度に実施した医療機器分野の実証における SBOM を用いた脆弱性管理のコスト評価結果を図 2-4 に示す。ここでは、対象とするソフトウェアが約 80 のコンポーネントを有しており、工数単価について¥10,000/時間と仮定している。また、SBOM による管理は、SBOM ツールを用いて実施した。手動でのコンポーネント管理の場合、手動でコンポーネントのリストを洗い出す必要があるほか、各コンポーネントに脆弱性が含まれるか、脆弱性情報データベース（NIST NVD 等）を手動で検索して確認する必要がある。そして、脆弱性が明らかになった際に各コンポーネント情報と脆弱性情報とを突合して影響有無を確認する必要がある。他方、SBOM による管理の場合、SBOM ツールの環境整備やツールの学習のための工数が必要となるが、コンポーネントの解析・特定を自動で行うことができるため、コンポーネントの解析・特定自体にはほとんど工数はかからない。新たな脆弱性が明らかになった場合、SBOM ツールに自動で反映され、その影響を受けるかをリアルタイムで特定することができるため、解析・特定結果に関する確認は必要となるものの、脆弱性管理にかかるコストを大幅に削減することができる。実証では、SBOM を活用した場合に要する工数が、手動での脆弱性管理と比較して 30%程度に低減されたことを確認した。なお、有償の SBOM ツールを用いた場合はツールのコストも追加される形となるが、対象とするコンポーネント数が多ければ多いほど、そのコストは按分されることに留意したい。

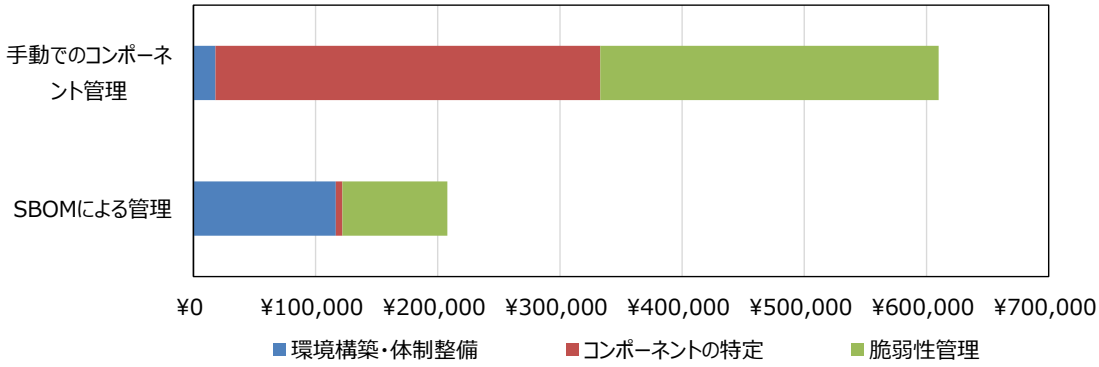

図 2-4 SBOM 管理による脆弱性管理コストの低減結果
（医療機器分野における 2022 年度の実証結果より）[9]

SBOM 導入による脆弱性管理に対する間接的なメリットとして、脆弱性のリスクが低減されることで製品価値や企業価値が向上するほか、大局的には、脆弱性の少ない製品が増えることで、サイバー空間全体のセキュリティが向上するというメリットも存在する。

SBOM 導入によるメリットの 2 つ目として、ライセンス管理上のメリット、すなわち、ソフトウェアに含まれるコンポーネントのライセンスを識別し、各ライセンスの要求事項に従った対応をするという一連のプロセスにおけるメリットが挙げられる。近年のソフトウェアの多くは OSS を含んでいるが、OSS のライセンスに違反した場合、ソフトウェアの販売停止や回収、罰金の支払い、企業ブランドイメージの低下等、大きな影響を受ける可能性がある。海外では、OSS ライセンス違反による訴訟事例が複数存在し、例えば、2009 年に家電メーカーら 14 社が GNU General Public License（GPL）違反で起訴された事例、2013 年にメディアプレイヤーメーカーが GPL 違反で起訴された事例、2021 年にテレビメーカーが GPL 違反で起訴された事例等が挙げられる。OSS を利用する場合、ライセンスの種類に応じた適切な対応が必要であり、例えば GPL の場合、派生物も GPL が適用されるほか、GPL を他のソフトウェアと組合せて新たなソフトウェアを作成し頒布した場合、当該ソフトウェアは全体として GPL が課す条件 に従わなければならない。また、Mozilla Public License（MPL）の場合、GPL と同様に派生物も MPL が適用される一方で、組合せて作成した新たなソフトウェアに対しては MPL が適用されない。そのため、OSS を利用する場合、自らの責任ですべての OSS のライセンスを確認し、それぞれのライセンスに準拠する必要があるが、OSS のライセンス情報を抜け漏れなく管理することは容易ではない。SBOM を導入し、ライセンス情報も含めてコンポーネントを管理することで、ライセンス違反のリスクを低減することができるほか、脆弱性管理と同様に、ライセンス管理にかかるコストを低減することができる。さらには、ライセンス違反に起因する財務リスクから組織を保護することができ、製品価値や企業価値の向上に寄与する。

SBOM 導入によるメリットの 3 つ目として、ソフトウェア開発ライフサイクル（SDLC）が改善し、開発生産性が向上するというメリットが挙げられる。ソフトウェア開発初期段階から SBOM を生成することで、

[9] SBOM ツールのコストは含まず。また、「脆弱性管理」について、脆弱性の特定とリスク評価に関する工数までを考慮し、工数が SBOM の有無によって大きく変動しない脆弱性の修正作業や報告作業等は含めていない。

コンポーネントに含まれる既知の脆弱性やライセンスの問題等のコンポーネントに関する問題に予め対応することができる。これらの問題を早期に特定することで、開発遅延の発生を防ぐことができるほか、対応コストを低減することができる。また、社内で利用が承認されたコンポーネントの情報を SBOM として管理しておくことで、開発の際に毎度コンポーネントを調査・承認する必要がなくなり、結果として開発工数の低減が期待できる。開発生産性向上のメリットに関して、Linux Foundation が 2021 年の第 3 四半期にグローバルの 412 の組織を対象に実施した調査[10]によれば、SBOM のメリットについて、回答組織の 51%が「開発者がより広範で複雑なプロジェクト間の依存関係を理解しやすくなる」ことを挙げており、これは脆弱性管理のメリット（同 49%）やライセンス管理のメリット（同 44%）より高い割合となっている。

本節では、SBOM 導入による代表的なメリットとして、脆弱性管理のメリット、ライセンス管理のメリット、開発生産性向上のメリットの 3 つを挙げたが、それ以外にも想定されるメリットは存在する。例えば、SBOM による管理を行うことで、ソフトウェアの EOL 管理が容易となることも挙げられる。SBOM 導入により様々なメリットを享受しうるが、どのようなメリットを特に重視するかは、自組織において SBOM 導入により解決したい課題と、SBOM 導入の目的を踏まえて検討する必要がある。

コラム：Log4j の脆弱性（Log4Shell）に対する SBOM 導入の効果

2021 年 12 月、ログ出力ライブラリの Apache Log4j において任意コード実行の脆弱性（通称：Log4Shell）が発見された。OSS の Log4j は無償で利用可能であり、様々な機能が内包されていたことから、Java システムにおけるログ出力の定番的なモジュールとして様々な用途に用いられていた。しかしながら、発見された脆弱性を悪用し、Log4j が動作するアプリケーションに対して不正アクセスを行うことで、情報漏えいやマルウェア感染等の被害につながるおそれがある。米国 CISA 等が発表した「2021 年に頻繁に悪用された脆弱性」[11]では、2021 年 12 月に発見された脆弱性に関わらず Log4Shell が 1 位にランクインしており、この脆弱性の影響範囲は計り知れない。

Log4Shell の脆弱性が広く悪用されている理由として、多数のソフトウェアに導入されていることや攻撃が容易であることのほかに、コンポーネントとして組み込まれているため、サプライヤーやソフトウェア利用者が脆弱性の影響に気づかず、対策が実施されていないことも挙げられる。

具体的には、

図 **2-5** に示すように、ソフトウェア利用者が確認できる（認識している）コンポーネントの範囲より深くに Log4j のコンポーネントが存在する場合、ソフトウェア利用者は認識していないものの Log4j の脆弱性が悪用され、ソフトウェア利用者に影響を及ぼす可能性がある。

複数階層のコンポーネントを含む SBOM を導入することで、Log4j の脆弱性が発見された際に、利

[10] 脚注 2 参照。

[11] CISA, Alert (AA22-117A) 2021 Top Routinely Exploited Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

用しているソフトウェアが影響を受けるかを即座に確認でき、脆弱性対応を迅速化することができる。これにより、脆弱性が悪用されることのリスクが低減されるほか、脆弱性対応や影響範囲の特定に要するコスト低減にも寄与する。

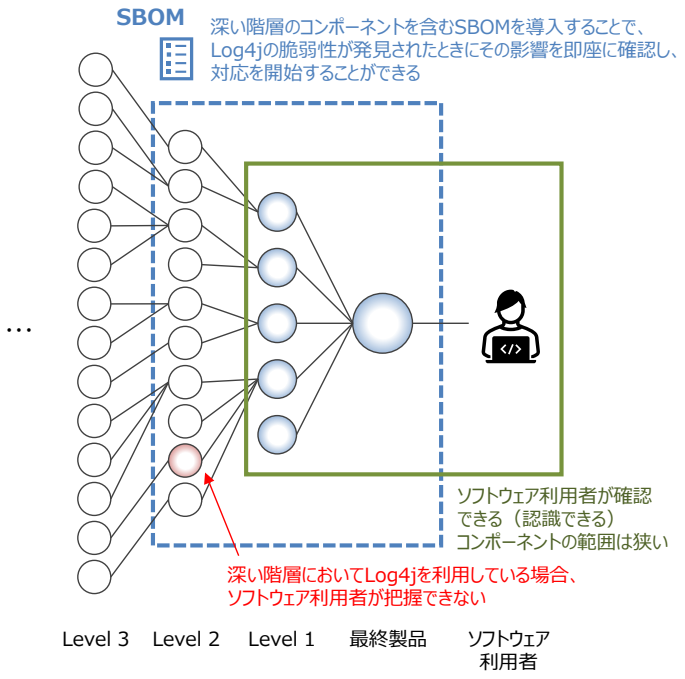

図 2-5 ソフトウェアのコンポーネント階層のイメージ

2.3. SBOM の「最小要素」

2021 年 5 月の米国大統領令を受け、NTIA は 2021 年 7 月に SBOM の「最小要素」の定義に関する文書を公開した[12]。NTIA が定める「最小要素」の定義には、SBOM に含めるべき情報に関するカテゴリーである「データフィールド」だけではなく、SBOM を導入する組織が考慮すべきカテゴリーとして「自動化サポート」、「プラクティスとプロセス」のカテゴリーも規定されている。具体的な「最小要素」のカテゴリーと定義は表 2-3 に示すとおりである。

[12] NTIA, The Minimum Elements For a Software Bill of Materials (SBOM)
https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

表 2-3 米国 NTIA による SBOM の「最小要素」の定義

カテゴリー名称	概要	定義
データフィールド（Data Fields）	各コンポーネントに関する基本情報を明確化すること	以下の情報を SBOM に含めること。 ● サプライヤー名 ● コンポーネント名 ● コンポーネントのバージョン ● その他の一意な識別子 ● 依存関係 ● SBOM 作成者 ● タイムスタンプ
自動化サポート（Automation Support）	SBOM の自動生成や可読性等の自動化をサポートすること	SBOM データは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWID タグを用いること。
プラクティスとプロセス（Practices and Processes）	SBOM の要求、生成、利用に関する運用方法を定義すること	SBOM を利活用する組織は、以下の項目に関する運用方法を定めること。 ● SBOM の作成頻度 ● SBOM の深さ[13] ● 既知の未知[14] ● SBOM の共有 ● アクセス管理 ● 誤りの許容[15]

SBOM の利活用においては、コンポーネントに関する情報を収集し、一貫性のあるデータ構造を確立することが必要不可欠となる。そのため、データフィールドのカテゴリーでは、SBOM の対象となるコンポーネントを一意に特定するための情報を含めることが「最小要素」として位置づけられている。具体的なデータフィールドの定義は表 2-4 に示すとおりであり、SBOM の対象となるコンポーネントの名称やバージョン、その他の識別子に関する情報だけでなく、当該コンポーネントのサプライヤー及び SBOM 作成者の名称、コンポーネントの依存関係及びタイムスタンプに関する項目が含まれる。

---

[13] 図 2-9 に示すように、ソフトウェアのコンポーネントは階層構造となっていることが多い。SBOM の深さとは、この階層構造において、どの深さのコンポーネントまで SBOM に含めるか、ということを指す。

[14] 作成した SBOM において完全なコンポーネントの依存関係が未知である場合に、未知であるという事実を明示するということを意味する。例えば、依存関係の存在が不明であることの明示、部品を特定できていない範囲の明示等が挙げられる。

[15] NTIA は、「ソフトウェアサプライチェーンの管理方法は日々進化しているため、SBOM を導入・運用する初期フェーズにおいて完全性が欠如する可能性がある」としており、その上で、「偶発的な誤りに対しては明確に許容すべきである」としている。これにより、ツールの継続的な改善が促進されるとしている。

表 2-4 「最小要素」として SBOM に含めるべきデータフィールド

項目	説明
サプライヤー名（Supplier Name）	コンポーネントを開発、定義及び識別するエンティティの名称。
コンポーネント名（Component Name）	サプライヤーによって定義された、ソフトウェアのある単位に対する名称。
コンポーネントのバージョン（Version of the Component）	コンポーネントを識別するために使用されるバージョンに関する識別子。
その他の一意の識別子（Other Unique Identifiers）	コンポーネントを識別するために使用される又は関連するデータベースの検索キーとして機能するその他の識別子。
依存関係（Dependency Relationship）	コンポーネントがあるソフトウェアに含まれているという関係性の特徴づけの情報。
SBOM 作成者（Author of SBOM Data）	コンポーネントの SBOM を作成するエンティティの名称。
タイムスタンプ（Timestamp）	SBOM データを作成した日付と時刻の情報。

2.4. SBOM フォーマットの例

SBOM の「最小要素」に規定されているとおり、SBOM データは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されることが求められる。この際、共通的なフォーマットを用いることで組織内の管理が効率化されるほか、組織を越えて SBOM を共有する際の相互運用性が高まり、ソフトウェアサプライチェーンの透明性向上に寄与する。使用されうる SBOM フォーマットの例として、以下に示す 3 つのフォーマットが挙げられる。

(1) SPDX[16]

(2) CycloneDX

(3) SWID タグ（Software Identification タグ）

SPDX の特徴として、スニペット、ファイル、パッケージ、コンテナ、OS ディストリビューション等の幅広いソフトウェア部品タイプをサポートしているほか、コンポーネントのライセンス情報を一意に特定するための識別

[16] SPDX v2.3 までは Software Package Data Exchange の略称で SPDX が用いられていたが、2024 年 4 月に発行された SPDX v3.0 では、System Package Data Exchange を意味するものとして定義されている

子のリストが用意されていることが挙げられる。SPDX の項目のうち、プロセスマネジメント標準などで必要となる SBOM としての要素を満たす程度に最低限必要な項目のみを含んだ SPDX Lite という日本発のフォーマットも存在する。SPDX Lite は、簡易的な SBOM 作成・管理を行う際に優れているほか、日本語で作成された仕様書等のドキュメントが豊富であることも特徴の一つである。CycloneDX はセキュリティ管理を念頭に置いたフォーマットであり、対象となるソフトウェアの情報だけでなく、ソフトウェアに含まれる既知の脆弱性に関する情報やその脆弱性の悪用可能性に関する情報も記述することが可能である。最後に、SWID タグについて、ソフトウェアのライフサイクルに沿って SBOM を管理することができる特徴がある。

本節では、図 2-1 で示した簡易シナリオを再度考え、それぞれの SBOM フォーマットで A 社が作成する SBOM の例を示す。

(1) SPDX

SPDX は Linux Foundation の傘下のプロジェクトによって開発された SBOM フォーマットで、2021 年 9 月には ISO/IEC 5962:2021 として国際標準化された。SPDX フォーマットにおける SBOM では、SPDX Specification にしたがって作成されたコンポーネントやライセンス、コピーライト等の情報が記載され、Tag-Value(txt)形式、RDF 形式、xls 形式、json 形式、YAML 形式、xml 形式がサポートされている。SPDX のフォーマットの構成、使用例・使用目的、特徴については付録の 10.3.3(1)を参照のこと。

前述した簡易シナリオにおいて、Tag-Value 形式の SPDX v2.3.0 フォーマットを用いて A 社が SBOM を作成した場合、図 2-6 のような SBOM が作成される。ここで、色の関係は、表 2-1 で示した SBOM の概念的イメージと、SPDX フォーマットにおける項目との対応関係を示している。表 2-5 に示すとおり、SBOM の「最小要素」の各項目に対して、SPDX フォーマットの項目は対応可能である。

#	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in Application	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in Browser	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in Application	Company A	05-09-2022 13:00:00

SPDXフォーマット（tag-value形式）のSBOM

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aefb-fc10d9ac1eed
DocumentName: SBOM Example
SPDXID: SPDXRef-DOCUMENT
Creator: Organization: Company A
Created: 2022-05-09T13:00:00Z
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Application-v1.1

PackageName: Application
SPDXID: SPDXRef-Application-v1.1
PackageVersion: 1.1
PackageSupplier: Organization: Company A
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageChecksum: SHA1: 75068c26abbed3ad3980685bae21d7202d288317
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
ExternalRef: SECURITY cpe23Type cpe:2.3:a:company_a:application:1.1:*:*:*:*:*:*:*
Relationship: SPDXRef-Application-v1.1 CONTAINS SPDXRef-Browser-v2.1
Relationship: SPDXRef-Application-v1.1 CONTAINS SPDXRef-Protocol-v2.2

（以下省略）
```

図 2-6 簡易シナリオにおける SPDX フォーマット（Tag-Value 形式）の SBOM 例

表 2-5 SBOM「最小要素」に対応する SPDX の項目

SBOM「最小要素」のデータフィールド	対応する SPDX の項目
サプライヤー名（Supplier Name）	PackageSupplier
コンポーネント名（Component Name）	PackageName
コンポーネントのバージョン（Version of the Component）	PackageVersion
その他の一意の識別子（Other Unique Identifiers）	DocumentNamespace と SPDXID の組合せ、ExternalRef
依存関係（Dependency Relationship）	Relationship（DESCRIBES; CONTAINS による表現）
SBOM 作成者（Author of SBOM Data）	Creator

SBOM「最小要素」のデータフィールド	対応する SPDX の項目
タイムスタンプ（Timestamp）	Created

SPDX は、OSS のライセンスコンプライアンスに関する情報を効果的に扱うために開発されたフォーマットであり、ファイルのレベルまで構造化して詳細な情報を表現できる点が特徴である。また、対象となるコンポーネントについて、スニペットやファイルに留まらず、パッケージ、コンテナ、OS ディストリビューションまで拡張可能である。自動処理を意図して開発されたフォーマットであり、前述のとおり、ISO/IEC 5962:2021 として国際標準化されていることも大きな特徴である。

SPDX の項目のうち、プロセスマネジメント標準などで必要となる SBOM としての要素を満たす程度に最低限必要な項目のみを含んだ SPDX Lite という日本発のフォーマットも存在する。SPDX Lite は、手作業によりライセンス情報を作成する組織において、SPDX 準拠のライセンス情報が膨大で運用が困難な場合に、必要な情報のみ授受する場合を想定して設計されている。OpenChain Japan Work Group（WG）のライセンス情報サブグループによって開発され、SPDX のサブセットとして、ISO/IEC 5962:2021 規格の一部にも含まれている。SPDX Lite フォーマットにおける SBOM では、コンポーネントやライセンス、コピーライト等の情報が記載され、Tag-Value(txt)形式、RDF 形式、xls 形式、json 形式、YAML 形式、xml 形式がサポートされている。SPDX Lite のフォーマットの構成、使用例・使用目的、特徴については付録の 10.3.3(1)を参照のこと。

前述した簡易シナリオにおいて、xls 形式の SPDX Lite フォーマットを用いて A 社が SBOM を作成した場合、図 2-7 のような SBOM が作成される。xls 形式の SPDX Lite フォーマットの場合、一つの xls ファイルに「Creation Information」と「Package Information」の 2 つのシートを含めることで、SBOM 情報を記載することができる。ここで、色の関係は、表 2-1 で示した SBOM の概念的イメージと、SPDX Lite フォーマットにおける項目との対応関係を示している。表 2-6 に示すとおり、SBOM の「最小要素」の「依存関係（Dependency Relationship）」以外の項目に対して SPDX Lite フォーマットの項目は対応可能である。

#	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in Application	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in Browser	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in Application	Company A	05-09-2022 13:00:00

SPDX-Liteフォーマット（xls形式）のSBOM

Creation Information Sheet

SPDX Version	SPDX-2.2
Data License	CC0-1.0
SPDX Identifier	SPDXRef-DOCUMENT
Document Name	SBOM Example
SPDX Document Namespace	http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aefb-fc10d9ac1eed
Creator	Company A
Created	05-09-2022 13:00:00

Package Information Sheet

PackageName	PackageSPDXIdentifier	PackageVersion	PackageFileName	PackageSupplier	PackageDownloadLocation	FilesAnalyzed	PackageHomePage	ConcludedLicense	DeclaredLicense	Comments on License	Copyright Text	Package Comment	External Reference field
Application	234	1.1	省略	Company A	省略								
Browser	334	2.1		Company B									
Compression Engine	434	3.1		Mr. C									
Protocol	534	2.2		Community P									

図 2-7 簡易シナリオにおける SPDX Lite フォーマット（xls 形式）の SBOM 例

表 2-6 SBOM「最小要素」に対応する SPDX Lite の項目

SBOM「最小要素」のデータフィールド	対応する SPDX Lite の項目
サプライヤー名（Supplier Name）	PackageSupplier
コンポーネント名（Component Name）	PackageName
コンポーネントのバージョン（Version of the Component）	PackageVersion
その他の一意の識別子（Other Unique Identifiers）	SPDX Identifier と SPDX Document Namespace の組合せ、PackageSPDX Identifier
依存関係（Dependency Relationship）	-
SBOM 作成者（Author of SBOM Data）	Creator
タイムスタンプ（Timestamp）	Created

SPDX Lite は、SPDX から必要最低限の項目のみを抽出したフォーマットであるため、運用性を重視した SBOM 管理が可能となる。SPDX は記述する必要がある項目が多く、自動処理による管理を目的としているが、SPDX Lite は項目数が限られるため、手作業での管理も現実的に可能となる。ただし、SPDX Lite には必要最低限の項目のみが含まれているため、例えば NTIA の「最小要素」で規定されている「依存関係」に関する項目等は表現できないことに注意が必要である。項目数が限定的であるため、サプライチェーン内で SBOM 共有を行う際に上流組織が求める要件に合致しない可能性もあり、SPDX Lite の利用可否の判断においては、取引先への確認を行う等の対応が望まれる。さらに、SPDX Lite フォーマットの SBOM を手作業で管理する場合、自動管理の場合と比較して管理工数が大きくなる場合があることにも注意が必要である。

(2) CycloneDX

CycloneDX は、セキュリティに特化した SBOM フォーマットの標準を開発することを目標とし、OWASP コミュニティのプロジェクトによって開発された SBOM フォーマットである。CycloneDX フォーマットによる SBOM では、コンポーネントやライセンス、コピーライト等の情報が記載され、json 形式、xml 形式、Protocol Buffers (protobuf)形式がサポートされている。CycloneDX のフォーマットの構成、使用例・使用目的、特徴については付録の 10.3.3(3)を参照のこと。

前述した簡易シナリオにおいて、xml 形式の CycloneDX v1.5 フォーマットを用いて A 社が SBOM を作成した場合、図 2-8 のような SBOM が作成される。ここで、色の関係は、表 2-1 で示した SBOM の概念的イメージと、CycloneDX フォーマットにおける項目との対応関係を示している。表 2-7 に示すとおり、SBOM の「最小要素」の各項目に対して CycloneDX フォーマットの項目は対応可能である。

#	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in Application	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in Browser	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in Application	Company A	05-09-2022 13:00:00

CycloneDXフォーマット（XML形式）のSBOM

```
<?xml version="1.0" encoding="utf-8"?>
<bom xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 serialNumber="urn:uuid:3e671687-395b-41f5-a30f-a58921a69b71" version="1"
 xmlns="http://cyclonedx.org/schema/bom/1.3">
 <metadata>
  <timestamp>2022-05-09T13:00:00Z</timestamp>
  <authors>
   <author>
    <name>Company A</name>
   </author>
  </authors>
  <component type="application">
   <name>Application</name>
   <version>1.1</version>
   <hashes>
    <hash alg="SHA-1">75068c26abbed3ad3980685bae21d7202d288317</hash>
   </hashes>
   <cpe>cpe:2.3:a:company_a:application:1.1:*:*:*:*:*:*:*</cpe>
   <externalReferences />
   <components />
  </component>
  <manufacture>
   <name>Company A</name>
  </manufacture>
  <supplier>
   <name>Company A</name>
  </supplier>
 </metadata>

  (中略)

 <dependencies>
  <dependency ref="pkg:maven/org.company_b/browser@2.1">
   <dependency ref="pkg:maven/org.c/CompressionEng@3.1" />
  </dependency>
  <dependency ref="pkg:maven/org.community_p/protocol@2.2" />
 </dependencies>

  (以下省略)
```

図 2-8 簡易シナリオにおける CycloneDX フォーマット（xml 形式）の SBOM 例

表 2-7 SBOM「最小要素」に対応する CycloneDX の項目

SBOM「最小要素」のデータフィールド	対応する CycloneDX の項目
サプライヤー名（Supplier Name）	component/supplier/name

SBOM「最小要素」のデータフィールド	対応する CycloneDX の項目
コンポーネント名（Component Name）	component/name
コンポーネントのバージョン（Version of the Component）	component/version
その他の一意の識別子（Other Unique Identifiers）	serialNumber、component/cpe
依存関係（Dependency Relationship）	dependencies/dependency ref
SBOM 作成者（Author of SBOM Data）	metadata/authors/author/name
タイムスタンプ（Timestamp）	metadata/timestamp

CycloneDX の特徴として、セキュリティ管理を念頭に置いた SBOM フォーマットであることが挙げられる。2022 年 1 月にリリースされた CycloneDX Version 1.4 ではオブジェクトモデルに「Vulnerabilities」が追加され、SBOM に含まれるサードパーティソフトウェアや OSS に存在する既知の脆弱性と、その脆弱性の悪用可能性を記述できるフォーマットとなっている。また、SPDX と同様に、ツールによる自動処理を目的としたフォーマットである。

(3) SWID タグ（Software Identification タグ）

SWID タグは、組織が管理対象とするデバイスにインストールされたソフトウェアを追跡することを目標として開発された。2012 年に ISO で定義され、2015 年に ISO/IEC 19770-2:2015 として更新された。SWID タグでは、ソフトウェアライフサイクルに沿ったソフトウェアのインストールプロセスの一貫として、デバイスにソフトウェアがインストールされるとタグと呼ばれるインストールされたソフトウェアの情報がデバイスに付与され、アンインストールされるとタグが削除される。SWID タグフォーマットによる SBOM では、SWID タグにしたがって作成されたデバイスにインストールされたソフトウェアやソフトウェアに適用したパッチ等の情報が記載され、xml 形式がサポートされている。SWID タグは、対象とするデバイスのライフサイクルを把握するために、デバイスにインストールされたソフトウェアの情報を示すタグが規定されている。各タグでは、タグの作成者、デバイスにインストールされるソフトウェア、他のソフトウェアへのリンクによる依存関係等の情報を提示することができ、対象とするデバイスの SBOM として使用することが可能である。SWID タグのフォーマットの構成、使用例・使用目的、特徴については付録の 10.3.3(4)を参照のこと。

前述した簡易シナリオにおいて xml 形式の SWID タグを用いて A 社が SBOM を作成した場合、図 2-9 のような SBOM が作成される。ここで、色の関係は、表 2-1 で示した SBOM の概念的イメージと、SWID タグフォーマットにおける項目との対応関係を示している。表 2-8 に示すとおり、SBOM の「最小要素」の各項目に対して SWID タグフォーマットの項目は対応可能である。

#	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in Application	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in Browser	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in Application	Company A	05-09-2022 13:00:00

SWIDタグフォーマット（XML形式）のSBOM

```
<SoftwareIdentity
 xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
 xmlns:sha512="http://www.w3.org/2001/04/xmlenc#sha512"
 name="application"
 tagId="Company A/application@1.1"
 version="1.1">
 <Entity name="Company A" role="tagCreatorsoftwareCreator" />
 <Meta title="Company A Application v1.1" timestamp="2022-05-09T13:00:00Z" />
 <Link href="swid:Company B/browser@2.1" rel="component" />
 <Link href="swid:Community P/ptotocol@2.2" rel="component" />
 <Payload >
  <File name="Company-A-application-1.1.exe"
sha512:hash="BC55DEF84538898754536AE47CC907387B8F61D9ACD7D3FB8B8A624199682C8FBE6D163108
8AE6A322CDDC4252D3564655CB234D3818962B0B75C35504D55689"/>
 </Payload>
</SoftwareIdentity>

（以下省略）
```

図 2-9 簡易シナリオにおける SWID タグフォーマット（xml 形式）の SBOM 例

表 2-8 SBOM「最小要素」に対応する SWID タグの項目

SBOM「最小要素」のデータフィールド	対応する SWID タグの項目
サプライヤー名（Supplier Name）	<Entity> @role(tagCreator) @name
コンポーネント名（Component Name）	<SoftwareIdentity> @name
コンポーネントのバージョン（Version of the Component）	<SoftwareIdentity> @version
その他の一意の識別子（Other Unique Identifiers）	<SoftwareIdentity>@tagId
依存関係（Dependency Relationship）	<Link> @rel @href
SBOM 作成者（Author of SBOM Data）	<Entity> @role(softwareCreator) @name
タイムスタンプ（Timestamp）	<Meta> @timestamp

SWID タグはソフトウェア識別に関するフォーマットであるが、コンポーネントのライセンスの情報や、パッチやアップデートに関する情報、脆弱性や脅威に関する情報等、セキュリティに関する情報も含めること

ができるフォーマットである。

ここまで、SPDX、SPDX Lite、CycloneDX、SWID タグにおける SBOM 例を示したが、多くのフォーマットは SBOM ツールを用いた自動処理・管理を目的としている。SBOM ツールを用いてソフトウェアのソースコードやバイナリファイルをスキャンし、ソフトウェアに含まれるコンポーネントを自動検出することで、自動で SBOM を作成することができる。加えて、SBOM ツールによっては、脆弱性情報やライセンス情報を継続的に把握することができるため、管理業務を効率化することができる。そのため、SBOM を導入する組織は、SBOM ツールを用いた SBOM の作成・管理を行うことが現実的である。代表的な SBOM ツールは付録の 10.3.2 に示すとおりであり、有償の SBOM ツールだけでなく、無償の SBOM ツールも公開されている。

SBOM を導入する組織は、自組織の SBOM 導入の目的や SBOM 適用範囲を踏まえて SBOM ツールの選定の観点を整理した後、当該観点に基づき、複数の SBOM ツールを評価し、選定することが望まれる。SBOM ツールの選定に当たって実施すべき事項や認識しておくべきポイントは 4.2 を参照のこと。

SBOM ツールを用いた SBOM 管理を行う場合、図 2-6～図 2-9 に示したような Tag-Value 形式や xml 形式の SBOM ドキュメントはあまり意識せず、SBOM を作成・管理することができる。特に、多くの有償の SBOM ツールではダッシュボード機能が充実しているため、SBOM に含まれるコンポーネント一覧を簡単に表示できるほか、各コンポーネントの脆弱性やライセンスコンプライアンスに関する情報も一覧表示やグラフ表示することができる。

2.5. SBOM に関する誤解と事実

SBOM 導入のメリットがあるものの、国内における SBOM の普及率は高いとは言えない。この理由として、SBOM 導入にかかるコストの課題、技術的な課題、人材に関する課題等の様々な課題が考えられるが、このほかにも SBOM の効果や位置づけが適切に認知されていない課題も存在する。このような課題に対し、米国 NTIA は 2021 年に「SBOM Myths vs. Facts」[17]（SBOM の神話と事実）という文書を発表し、SBOM に関する誤解と事実を明らかにした。NTIA の文書で示された誤解と事実の概要は以下のとおりである。

誤解：SBOM は攻撃者を支援する

（事実）SBOM が攻撃に利用される可能性はあるものの、SBOM により透明性を確保することによる「攻撃者からの防御」におけるメリットの方が大きい。攻撃者にとって、SBOM やソフトウェアの透明性に関する情報の効果は限定的であり、一般的に攻撃者は SBOM を必要としない。例え

[17] NTIA, SBOM Myths vs. Facts
https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf

ば、WannaCry によるランサムウェア攻撃は、攻撃のための前提条件として SBOM は必要ではない。

誤解：SBOM だけでは有用・実用的な情報を得ることができない

（事実）SBOM は、ソフトウェアのサプライヤー、利用者、運用者をサポートする。例えば、利用者がソフトウェアに対する攻撃を受けたとき、SBOM を使用することで攻撃の影響を受けているか、攻撃の影響範囲はどこかを容易に判断できる。また、SBOM に基づくコンポーネント情報があることで、ソフトウェアの透明性が向上し、管理が容易となる。

誤解：SBOM は公開しなければならない

（事実）SBOM を公開する必要はなく、SBOM 作成者やサプライヤーの判断で SBOM の共有方法を判断することができる。米国大統領令においても、SBOM の公開は SBOM 作成者の判断であり、必須ではないことが明確に記載されている。

誤解：SBOM は知的財産や企業秘密を露呈する

（事実）SBOM はソフトウェアに含まれているコンポーネントの一覧リストであり、特許やアルゴリズムは含まれておらず、知的財産を公開するものではない。SBOM は単なる「材料の一覧」であり、特許やアルゴリズムのような「レシピ」とは異なる。また、SBOM には、ソフトウェアのソースコード自体は含まれない[18]。第三者が開発したコンポーネントの特許やアルゴリズム等の知的財産は、コンポーネントの開発者又は著作権所有者に帰属することに留意する必要がある。

誤解：SBOM の導入を支援するプロセスは存在しない

（事実）ソフトウェア構成分析ツールは、一部の分野では、10 年以上にわたって企業内で使用されてきた実績がある。ソフトウェアの透明性に関しては、NTIA の活動、大統領令、SBOM フォーマットの標準化等の活動が進んでいるほか、一部の分野では、ソフトウェアの透明性について 5 年以上にわたって議論や実証の取組が進められており、他分野での導入をサポートしている。

また、国内で 2022 年度に実施した実証等を通じ、以下に示すさらに具体的な誤解と事実が明らかとなった。

誤解：対象ソフトウェアが直接利用しているコンポーネントのみ SBOM の管理対象とすればよい

（事実）対象ソフトウェアが直接利用しているコンポーネントだけでなく、そのコンポーネントが再帰的に利用するコンポーネントについても把握しないと、脆弱性対応が不十分となる可能性がある。どの階層のコンポーネントまで SBOM を作成するかという「SBOM の深さ」の観点に関しては、有識者による議論が進行中である。

誤解：SBOM 作成に用いる SBOM ツールの選定において、特に留意すべき点はない

（事実）SBOM 作成を支援するツールについて、有償のツール及び OSS として提供される無償

[18] SBOM にはソフトウェアのソースコードのような企業秘密は含まれないが、ソフトウェアプロバイダー、ベンダー等の情報など、他の専有情報が含まれる可能性があるため、適切な管理が必要であることに留意する必要がある。

のツールがすでに複数公開されている。無償のツールを活用することで、ツール自体はコストをかけずに入手できるものの、有償ツールと比較して、導入・活用に関するマニュアルやサポートが限定的であることが多く、ツールの習得に多大なコストがかかる可能性がある。また、有償ツールと比較してサポート範囲や性能が限定的であることが多く、SBOM 導入の目的を達成できない可能性もある。SBOM の作成に当たっては、SBOM ツールを活用することで効率的に SBOM を作成することができるが、自社の SBOM 導入の目的を踏まえて使用するツールを選定する必要がある。

誤解：SBOM ツールを活用することで、対象ソフトウェアに含まれるコンポーネントを完全に特定することができる

（事実）SBOM ツールを用いることで効率的に SBOM を作成することができるが、SBOM 作成に当たってのコンポーネントの誤検出や検出漏れが発生し、正確な SBOM を作成することができない場合もある。そのため、例えば、SBOM ツールにより出力された SBOM をレビューする等の取組も検討することが大切である。また、ランタイムライブラリのような実行時に動的に追加されるライブラリは、SBOM ツールがライブラリの実体を解析しないため、特定することができない。そのような場合は、パッケージマネージャー等を用いてライブラリに対する構成情報と実行環境を個別に用意し、SBOM ツールにそれを認識させることで再帰的なコンポーネントを特定できるようにする必要がある。

誤解：SBOM ツールが出力したすべての脆弱性に対応する必要がある

（事実）SBOM ツールが出力した脆弱性に関する結果を踏まえて脆弱性へのリスク対応を行う際、必ずしもすべての脆弱性が悪用可能ではなく、影響を受けない脆弱性も存在することに留意する必要がある[19]。そのため、脆弱性の影響範囲、リスクの評価結果、対応に要するコスト等を踏まえ、優先度を踏まえた脆弱性対応が必要となる。なお、手動での SBOM 管理の場合、脆弱性データベースを活用して脆弱性の有無を手作業で特定する必要があるほか、個別に脆弱性を評価し、さらに対応方針を個々に検討する必要があるため、膨大な管理コストを要する可能性がある。

誤解：作成する SBOM のコンポーネントの粒度はサプライチェーン全体で共通化し、必要なコンポーネント情報だけを保持するべきである

（事実）現状では、JVN や米国 NVD のような脆弱性情報データベースにおける「影響を受けるソフトウェア」の粒度が体系化されていないため、コンポーネントの粒度を限定すると脆弱性の特定で漏れが生じる可能性がある。そのため、OSS のみならず、自社製品等も含めてコンポーネント情報を保持することが有効である。

誤解：SBOM の対象はパッケージソフトウェアや組込ソフトウェアのみである

（事実）ソフトウェアに限らず、IT システムも SBOM の対象となりうる。なお、コンテナイメージに対する SBOM、SaaS ソフトウェアに対する SBOM、クラウドサービスに対する SBOM 等のオンラインアプリケーションに対する SBOM の議論も米国を中心に行われているが、クラウド環境特有の

[19] ある製品が既知の脆弱性の影響を受けるかどうかを示す機械判読可能なセキュリティ勧告の一つとして、VEX（Vulnerability Exploitability Exchange）が米国を中心に開発されている。

SBOM の課題も挙げられている。

誤解：SBOM のフォーマットとして、SPDX、CycloneDX、SWID タグの 3 つのフォーマットのみが認められており、独自フォーマットに基づく SBOM は認められない

（事実）米国 NTIA の定義に拠れば、SBOM とは「ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト」のことであり、独自フォーマットであってもこの定義に合致する場合は SBOM とみなすことができる。ただし、2.2 に記載のとおり、SBOM の「最小要素」として「自動化サポート」が位置づけられており、また、自動処理により効率化が図られることから、可能な限り、自動処理可能なフォーマットの採用を検討することが望ましい。

3. SBOM 導入に関する基本指針・全体像

3.1. SBOM 導入における基本指針

SBOM 導入に先立ち、SBOM を作成するソフトウェアの範囲を決定するとともに、SBOM を導入することで解決したい自組織の課題と、それを踏まえた SBOM 導入の目的を明確化することが必要である。例えば、膨大な数のコンポーネントが存在する大規模製品について、コンポーネントの依存関係も含めた SBOM を作成し、共有するという目的があった場合、有償の SBOM ツールを用いて SBOM を作成・管理することが想定される。また、コンポーネント数が膨大ではない小規模な製品について、最低限の項目のみ手作業でコンポーネントのバージョンを管理したいという目的であれば、SPDX Lite フォーマットを用いた SBOM を作成することが想定される。SBOM 導入の目的に応じて、作成すべき SBOM の項目、フォーマット、作成範囲、共有範囲等、SBOM の適用範囲が大きく異なるため、SBOM を導入する組織は、まず、SBOM 導入により解決したいソフトウェア管理に関する自社の課題を整理するとともに、SBOM 導入の目的を明確化した上で、SBOM を作成・運用・管理することが求められる。

3.2. SBOM 導入プロセス

SBOM 導入に関するプロセスは主に 3 つのフェーズに分けることができる。具体的には、SBOM 導入に関する環境構築・体制整備フェーズ、SBOM 作成・共有フェーズ、SBOM 運用・管理フェーズの 3 つである。それぞれのフェーズにおける主な実施項目・実施概要を図 3-1 に示す。

環境構築・体制整備フェーズでは、SBOM の導入範囲を明確化するとともに、SBOM の作成・共有に向け環境や体制を構築する。SBOM 作成・共有フェーズでは、実際に SBOM を作成するとともに、必要に応じて作成した SBOM を外部に共有する。SBOM はソフトウェア管理の一手法であるため、作成することが目的ではなく、SBOM を用いた管理が重要となる。よって、SBOM 運用・管理フェーズとして、SBOM の情報に基づき脆弱性管理やライセンス管理を行うとともに、SBOM 自体を適切に管理する必要がある。

以降の章では、各フェーズにおける主な実施事項や SBOM 導入に当たって認識しておくべきポイントを示す。

フェーズ	ステップ	実施概要
環境構築・体制整備フェーズ	SBOM適用範囲の明確化	SBOMの対象とするソフトウェアの情報（開発言語、契約形態、規制要求事項、社内の制約等）を整理して、SBOM適用範囲を明確化する。
	SBOMツールの選定	対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
	SBOMツールの導入・設定	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの導入・設定を行う。
	SBOMツールに関する学習	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの使い方を習得する。
SBOM作成・共有フェーズ	コンポーネントの解析	対象ソフトウェアのコンポーネントを解析するとともに、解析結果について、誤検出や検出漏れが無いかを確認する。
	SBOMの作成	作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
	SBOMの共有	対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する。
SBOM運用・管理フェーズ	SBOMに基づく脆弱性管理、ライセンス管理等の実施	脆弱性やライセンスに関するSBOMの情報を踏まえ、適切な脆弱性対応やライセンス管理対応を講じる。
	SBOM情報の管理	SBOMに含まれる情報やSBOM情報自体を適切に管理する。

図 3-1 SBOM 導入プロセス

4. 環境構築・体制整備フェーズにおける実施事項・認識しておくべきポイント

SBOM 導入に向け、まず SBOM に関する環境を整備するとともに、SBOM に関する体制を整備することが必要となる。本章では、環境構築・体制整備フェーズにおいて SBOM 導入組織が実施すべき事項や、SBOM 導入組織が認識しておくべきポイントを示す。

4.1. SBOM 適用範囲の明確化

【SBOM 導入に向けた実施事項】

- □ 対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する。
- □ 対象ソフトウェアの正確な構成図を作成し、SBOM 適用の対象を可視化する。
- □ 対象ソフトウェアの利用者及びサプライヤーとの契約形態・取引慣行を明確化する。
- □ 対象ソフトウェアの SBOM に関する規制・要求事項を確認する。
- □ SBOM 導入に関する組織内の制約（体制の制約、コストの制約等）を明確化する。
- □ 整理した情報に基づき、SBOM 適用範囲（5W1H）を明確化する。

【SBOM 導入に向け認識しておくべきポイント】

- 組織内外の開発者の知見を活用することで、対象ソフトウェアに関する効率的な情報収集を行うことができる。
- 対象ソフトウェアの正確な構成図を作成し、SBOM 適用の対象を可視化することで、リスク管理の範囲を明確化することができる。

SBOM 導入組織は、SBOM 導入により解決したい自社の課題と SBOM 導入の目的を踏まえ、SBOM の適用範囲を明確化する必要がある。SBOM 適用範囲は表 4-1 に示す 5W1H の観点に分類することができ、各観点において複数の適用項目（選択肢）が存在する。

表 4-1 SBOM 適用範囲（5W1H）

観点	主な適用項目（選択肢）
SBOM の作成主体（Who）	・ 自組織で SBOM を作成する ・ 取引契約のあるサプライヤーにて SBOM を作成する ・ 取引契約のないサプライヤー（OSS コミュニティ等）にて SBOM を作成する
SBOM の作成タイミング（When）	・ 製品計画又は開発計画時 ・ プログラム開発時 ・ ソフトウェアビルド時 ・ ソフトウェア納入時 ・ コンポーネントのバージョンアップ時
SBOM の活用主体（Who）	・ ソフトウェア利用者 ・ 最終製品ベンダー ・ 開発ベンダー ・ 最終製品ユーザー
SBOM の対象とするコンポーネントの範囲（What、Where）	・ 開発主体が直接利用するコンポーネントのみを対象とする ・ 既製品等開発委託契約のないコンポーネントから再帰的に利用されるコンポーネントも含めて対象とする
SBOM の作成手段（How）	・ 構成管理情報を踏まえて手動で SBOM を作成する ・ SBOM ツールを用いて自動で SBOM を作成する ・ 一部は構成管理情報を踏まえて手動で SBOM を作成、一部は SBOM ツールを用いて自動で SBOM を作成等、手動作成と自動作成を併用する
SBOM の活用範囲（Why）	・ 脆弱性管理 ・ ライセンス管理 ・ 開発生産性の向上 ・ 資産管理、トレーサビリティ ・ 利用者や納入先に対するコンポーネントに関する情報の共有
SBOM のフォーマット・項目（What）	・ 標準フォーマット（SPDX、SPDX Lite、CycloneDX、SWID タグ、SPDX Lite） ・ 米国大統領令におけるデータフィールドの最小要素 ・ 規制・要求事項や業界の慣行として使用される独自のフォーマット

SBOM 適用範囲は、これらの適用項目の組合せによって定まる。どの適用項目を選択するかにより、SBOM 導入に要するコストが異なることに留意が必要である。また、一つの観点に対し、複数の適用項

目を選択する可能性もある。適用項目の決定のために、SBOM の対象ソフトウェアに関する情報や、SBOM 導入に関する社内の制約を整理することが求められる。

対象ソフトウェアに関して、以下に関する情報をまず整理することが望まれる[20]。

- **開発言語**
  （例） Python、Java、Go、JavaScript、Rust、Swift、Objective-C、C、C++、VisualBasic 等
- **コンポーネントの形態**
  （例）ライブラリ、アプリケーション、ミドルウェア、データベースサービス 等
- **開発環境ツール**
  （例）Visual Studio、Eclipse、Android Studio、Xcode 等
- **ビルドツール**
  （例）Jenkins、Circle CI、Github Actions、Gradle、Maven 等
- **構成管理ツール**
  （例）Github、Gitlab、Team Foundation Server、Ansible 等
- **自組織で取扱うデータ形式**
  （例）ソースコード、パッケージ、コンテナ、バイナリデータ 等
- **動作環境**
  （例）OS、CPU アーキテクチャ 等

このような情報の整理においては、組織内外の開発者の知見を活用することが効果的である。特に、SBOM ツールを用いて SBOM を作成する場合、ツールによって対応している言語やコンポーネント形態が異なるため、開発言語とコンポーネントの形態については最低限把握することが必要である。そして SBOM の対象とするコンポーネントの範囲を明確化するために、対象ソフトウェアの構成を可視化することが望まれる。具体的には、対象ソフトウェアにおいて自組織で開発した範囲、取引契約のあるサプライヤーが開発した範囲、取引契約のないサプライヤーが開発した範囲（OSS 等）を可視化した図を作成することが望まれる。一例として、2022 年度の実証で対象とした歯科用 CT では以下のような構成図を作成し、この構成図をベースに、リスク管理の範囲を明確化した。

[20] 各項目に対する例示は網羅的ではなく、例示の内容に限定されないことに留意。

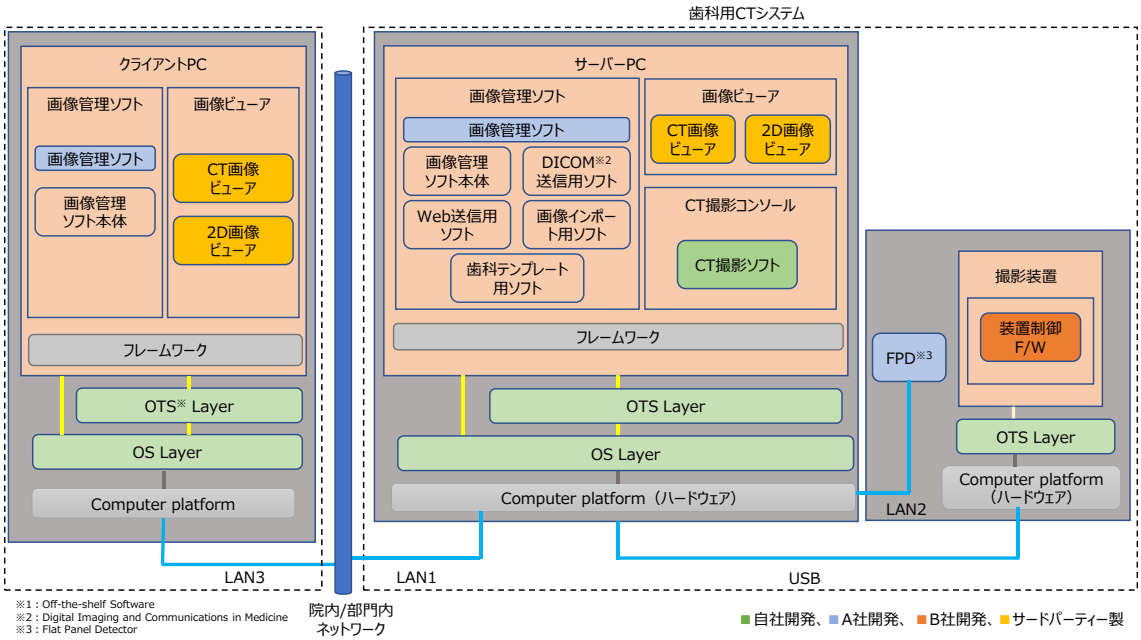

図 4-1 システム構成図の例（歯科用 CT の例）

あわせて、SBOM の対象とするコンポーネントの範囲対象を明確化するために、対象ソフトウェアの利用者及びサプライヤーとの契約形態・取引慣行を整理することが望まれる。具体的には、利用者・サプライヤーそれぞれについて、以下の各項目に関する対象ソフトウェアの情報を整理することが望まれる。

- **契約形態**：開発委託、製品販売 等
- **コンポーネント情報の提供**：提供なし、無償提供、要望された場合に提供可能 等
- **第三者コンポーネントの申告**：すべての OSS について申告、ライセンスを踏まえて一部の OSS について申告 等
- **脆弱性の通知**：修正すべきと判断された脆弱性に関してのみ通知 等
- **脆弱性の修正**：修正すべきと判断された脆弱性に関してのみ修正 等
- **納品形態**：バイナリパッケージ、機器組み込み、ライセンス情報（SaaS 等）、実行モジュール等
- **損害賠償責任**
- **知的財産権の帰属**：自社に帰属、納入先に帰属、納入元に帰属 等
- **改変の有無**：サードパーティから提供されたソフトウェアをそのまま使用している、自社にて改変して使用している 等

SBOM 適用項目のうち、SBOM のフォーマット・項目や SBOM の活用範囲を決定するために、対象ソフトウェアの SBOM に関する規制・要求事項を確認し、整理することが望まれる。現状のところ、

SBOM の提供が義務付けられているソフトウェアは限定的であるが、例えば米国では、政府調達対象となるソフトウェアベンダーに対して SBOM の提供を推奨している[21]ほか、EU では、2022 年 9 月に草案が発表されたサイバーレジリエンス法において、EU 市場に上市するデジタル製品に対する SBOM に関する要求事項が含まれている[22]。医療機器分野では、IMDRF（International Medical Device Regulators Forum：国際医療機器規制当局フォーラム）から発行された「医療機器サイバーセキュリティガイダンス（IMDRF ガイダンス）」を薬機法[23]による医療機器の規制に取り入れ 2023 年を目途に本格運用するとの方針が示されているところ、今後、規制の中で SBOM が要求される可能性もある。規制・要求事項において、SBOM のフォーマット・項目や SBOM の活用範囲が規定される可能性もあるため、対象ソフトウェアに関する規制・要求事項について随時情報収集し、求められる場合には具体的な要求事項を整理することが望まれる。

SBOM 適用項目の検討に当たっては、当然ながら、SBOM 導入に向けた組織内の制約も加味する必要がある。最も想定される制約としては、組織内の体制に関する制約やコストに関する制約が挙げられる。これらの制約が厳しい場合、限定的な SBOM 適用項目しか選択できない可能性もあるところ、SBOM 適用範囲の整理のために、予め組織内の制約を確認・整理することが望まれる。

整理したこれらの情報を踏まえ、上述した SBOM 適用範囲の 5W1H の各観点について、適用項目を検討・明確化することが望まれる。SBOM 適用範囲は対応したいリスクの範囲やレベルによって変わることに注意が必要である。例えば、将来的に規制・要求事項として求められる医療機器において SBOM を作成するとした場合に、自組織に限らず取引契約のあるサプライヤーにてソフトウェアビルド時に SBOM を作成し、その SBOM を利用者である医療機関が活用することが想定される。SBOM の対象とするコンポーネントの範囲としては、直接利用するコンポーネントに限らず、再帰的に利用されるコンポーネントも含めて対象とし、SBOM ツールを用いて自動で SBOM を作成することで、脆弱性管理及びライセンス管理に活用することが想定される。SBOM のフォーマット・項目としては、SPDX 等の自動処理可能なフォーマットに基づき、規制で求められる要求項目を含んだ SBOM を作成することが望まれる。

4.2. SBOM ツールの選定

【SBOM 導入に向けた実施事項】

□ 対象ソフトウェアの開発言語や組織内の制約を考慮した SBOM ツールの選定の観点を整理する。

---

[21] Office of Management and Budget, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[22] European Commission, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[23] 医療機器分野においては、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律

（選定の観点の例：機能、性能、解析可能な情報、解析可能なデータ形式、コスト、対応フォーマット、コンポーネント解析方法、サポート体制、他ツールとの連携、提供形態、ユーザーインターフェース、運用方法、対応するソフトウェア開発言語、日本語対応等）

□ 整理した観点に基づき、複数の SBOM ツールを評価し、選定する。

【SBOM 導入に向け認識しておくべきポイント】

- 複数の SBOM ツールの使い分けは非効率となる場合があるため、目的に対して最小限の SBOM ツールを用いた運用となるかどうか等も考慮することが望ましい。
- 有償の SBOM ツールは一般に高価である。一方で、無償の SBOM ツールは、ツール自体のコストは無料であるものの、環境整備や学習に当たっての情報が不足しており、導入・運用に大きな工数を要する可能性がある。
- 有償の SBOM ツールと比較して、無償の SBOM ツールの機能・性能は限定的である場合が多く、例えば、再帰的な利用部品が検出できない、読み込み可能な SBOM フォーマットに制限がある、ライセンスの検知漏れが発生する、導入環境が限定される等の課題がある。
- オンプレミス型の SBOM ツールでは、導入環境が制約される場合がある。また、SaaS 型の SBOM ツールでは、機密性の高いソースコードの情報が外部に送信される構造になっていないかを確認する必要がある。
- SBOM 導入が原因で開発効率が著しく下がることのないよう、既存の開発プロセスへの組込が容易な SBOM ツールを選定し、開発者に負担をかけない運用を心がけることが必要である。
- SBOM ツールの選定にあたり、無償トライアル等を利用して実際の使用感を体験することが効果的である。観点の設定や選定に難しさを感じる場合には、複数の SBOM ツールを扱う販売代理店に相談し、各ツールの特徴や長所・短所を比較評価しながら選定することも一案である。

SBOM 導入組織は、明確化した SBOM 適用範囲に対応する SBOM を作成するための環境構築・体制整備を行う必要がある。SBOM 作成・管理の環境として最も重要な設備は SBOM ツールである。SBOM を作成・管理するとした場合に、SBOM ツールは必ずしも必須ではなく、例えば SPDX Lite のように手動で SBOM を作成・管理できるフォーマットも用意されている。しかしながら、実証を通じて、SBOM ツールを活用することでコンポーネント管理にかかる工数は小さくなるほか、SBOM ツールを活用することで、OSS 間の依存関係や OSS の再利用も効率的に検出・管理でき、脆弱性発表から特定までのリードタイムを短縮可能であることが明らかとなった。そのため、SBOM ツールを用いた SBOM の作成・管理を行うことが現実的であり、本手引でも SBOM ツールを前提とした記載としている。

代表的な SBOM ツールは付録の 10.3.2 に示すとおりであり、SBOM ツールは大きく有償のツールと無償のツールに分かれる。有償の SBOM ツールは一般に高価であるが、ユーザーインターフェースが充実

しており、直感的な SBOM 作成・管理が可能であるほか、サポート体制が整備されているため、ツールの導入や運用に悩んだ際にベンダーや販売代理店に相談できるというメリットがある。さらには、各種開発ツールやコミュニケーションツールと連携可能な SBOM ツールも存在する。無償の SBOM ツールは、ツール自体のコストは無料であるものの、環境整備や学習に当たっての情報が不足していることが多い。そのため、ツールの導入・運用やエラー発生時の原因究明・対応に大きな工数を要する可能性がある。また、有償の SBOM ツールと比較して、無償の SBOM ツールの機能・性能は限定的であることが多く、例えば、再利用部品が検出できない、読み込み可能な SBOM フォーマットに制限がある、ライセンスの検知漏れが発生する、導入環境が限定される等の課題があるものの、無償の SBOM ツールは OSS コミュニティを中心に活発に開発されているため、機能・性能が向上していく可能性があることに留意する必要がある。なお、無償の SBOM ツールに関するサポートサービスを提供している企業もあり、無償の SBOM ツールを活用する場合に必要に応じて支援を受けることも想定される。

有償・無償の様々な SBOM ツールが用意されているところ、対象ソフトウェアの開発言語や組織内の制約を考慮した選定の観点を整理し、この観点に基づいて SBOM ツールを評価・選定することが望まれる。想定される選定の観点の例として、表 4-2 に示す観点が挙げられる。

表 4-2 SBOM ツールの選定の観点

観点	説明
機能	SBOM ツールが有する機能として、コンポーネントの解析機能、脆弱性情報・ライセンス情報の自動マッチング機能、リスクの定量化機能、依存関係や脆弱性情報等の可視化機能、脆弱性情報・ライセンス情報の自動追跡機能、新たな脆弱性が検出された際のアラート機能、アドバイザリー情報の自動レポート機能、SBOM データのインポート機能等が挙げられる。SBOM ツールによって対応している機能が異なるため、SBOM 導入の目的や SBOM 適用範囲を踏まえ、どの機能が必要であるかを整理することが望まれる。
性能	OSS の検出や脆弱性情報・ライセンス情報のマッチングに当たって、どの程度の誤検出・検出漏れが生じうるかは一つの重要な指標である。加えて、新たな脆弱性が見つかった際に、どれほど迅速にツールに反映されるかという点も重要となる。SBOM 導入の目的や SBOM 適用範囲を踏まえ、どの程度の性能[24]を求めるかを整理することが望まれる。

[24] なお、ツールの性能を把握する方法として、例えば、無償トライアルを利用して実際に解析するソフトウェアや利用する SBOM 等をツールに読み込ませ、正確な情報をツールが出力可能か確認することやツールベンダーがデータベースに収録している OSS や脆弱性の数、脆弱性情報の情報元（JVN、NVD 等）、データベースの更新頻度等の仕様を開発元・代理店に確認すること等が想定される。

観点	説明
解析可能な情報	SBOM ツールによって、解析できるコンポーネントの情報が異なる。有償ツールの多くはコンポーネントに関する脆弱性情報やライセンス情報を自動で解析できるほか、脆弱性情報の解析に特化したツールや、ライセンス情報の解析に特化したツールも存在する。SBOM 導入の目的や SBOM 適用範囲を踏まえ、どの情報が必要であるかを整理することが望まれる。
解析可能なデータ形式	SBOM ツールは、コンポーネント解析時に読込可能なデータ形式に条件がある。ファイル形式（拡張子別の対応可否）、対応するパッケージマネージャーの種類、ソフトウェアが動作可能な OS・CPU アーキテクチャ等、解析に使用するデータの形式を整理することが望まれる。
コスト	有償の SBOM ツールの場合、ツールのライセンス費用が必要となる。ツールによって料金体系は異なるが、多くのツールが年間のサブスクリプションモデルで提供している。オプションとして、複数の OSS 解析方法が利用できるツールがあるほか、問合せ対応に限らず OSS 管理に関する様々な相談が可能となるプランを提供しているツールも存在する。また、ライセンス費用の算出方法は、開発者数や組織の規模、解析コード量に応じた課金等、ツールによって様々であり、高額であっても会社全体で導入する場合にスケールメリットが出る場合もある。社内のコスト制約を踏まえ、SBOM ツールに対してどの程度のコストをかけることができるかを整理することが望まれる。
対応フォーマット	SBOM ツールによって、特定の SBOM フォーマット（SPDX、SPDX Lite、CycloneDX、SWID タグ等）の SBOM のみインポート可能／作成可能な場合がある。SBOM の作成に関しては、大半の SBOM ツールが複数の SBOM フォーマットをサポートしているが、SBOM のインポートに関しては、複数の SBOM フォーマットに対応している製品は多くない。SBOM 適用範囲を踏まえ、どの SBOM フォーマットに対応する必要があるかを整理することが望まれる。
コンポーネント解析方法	ソフトウェアに含まれるコンポーネントの解析方法は、コードマッチング、依存関係検出、文字列検出の大きく 3 つに大別できる。コードマッチングは、OSS データベースとのマッチングによって OSS を検出する方法であり、完全一致のコードマッチングのほか、スニペットマッチングと呼ばれる部分一致のコードマッチング方法も存在する。また、バイナリパターンによるマッチングを行う方法も存在する。依存関係検出は、パッケージマネージャーで取得する直接的・間接的な OSS を検出する方法であり、誤検出の発生可能性は低い。そして、文字列検出は、ソフトウェアのライセンス文字列を解析して、適用されているライセンスを検出する方法である。複数の解析方法を組合せて OSS 解析を行っている SBOM ツールもあれば、一部の解析方法のみに対応しているツールもあるため、SBOM 作成に当たって用意できるコード情報等を踏まえ、どの OSS 解析方法を採用すべきかを整理することが望まれる。

観点	説明
サポート体制	有償ツールに関しては、ツールの導入や運用についてベンダーに問合せが可能なSBOM ツールが存在するほか、オプションとして、ツールに関する問合せに限らずOSS 管理に関する様々な相談が可能となるプランを提供しているツールも存在する。また、無償ツールについても、サポートサービスを提供している企業もあり、必要に応じて支援を受けることも想定される。SBOM 適用範囲や組織内の SBOM 導入に関わる担当者の知識レベル等を踏まえ、どの程度のサポートが必要であるかを整理することが望まれる。
他ツールとの連携	開発環境、ビルドツール、ソフトウェアバージョン管理ツール、コミュニケーションツール等と連携可能な SBOM ツールが存在する。SBOM 作成の自動化等、ソフトウェア開発ライフサイクル全体の効率化を図る目的では、すでに組織内で活用しているツールとの連携ができることが望ましく、どのようなツールとの連携が必要であるかを整理することが望まれる。
提供形態	SBOM ツールの提供形態にはパッケージ版とクラウド版がある。パッケージ版のSBOM ツールを導入する場合、ツール料金のほかに、サーバの維持管理費用が発生する可能性があるほか、導入できる環境が制約される可能性がある。クラウド版の場合、パッケージ版と比較して初期導入にかかるコストや SBOM 共有に関する工数を低減できる。ただし、機密性の高い自社のソースコード情報が社外に送信されるおそれがないかを予め確認する必要がある。組織内のシステム制約を踏まえ、どちらの提供形態がふさわしいかを整理することが望まれる。
ユーザーインターフェース	SBOM ツールによって、CLI（コマンドラインインターフェース）のみ提供している場合と、GUI（グラフィカルユーザーインターフェース）も提供している場合がある。GUI 対応のツールの場合、直感的な SBOM の作成や出力結果の可視化が可能となる。SBOM 導入に関わる担当者の知識レベル等を踏まえ、どのようなユーザーインターフェースを備えたツールが求められるかを整理することが望まれる。
運用方法	開発者が自身で SBOM ツールによるコンポーネント解析を実行する場合は、開発環境と連携しバックグラウンドで自動的に解析が行われるような SBOM ツールを選定することで、開発者の負担を軽減することができる。一方、解析チームのような専門部隊が取り纏めて SBOM ツールを実行する場合は、ポリシー機能やライセンス等の補足情報が充実している SBOM ツールを選定することで、解析結果の精査がしやすくなる。
対応するソフトウェア開発言語	SBOM ツールによって対応しているソフトウェア開発言語が異なる。C、C++、Java、Python、Ruby、Swift、Go 等の代表的な言語であれば多くのツールが対応しているが、一部の言語については、対応しているツールが限定的な場合がある。対象ソフトウェアの情報整理結果を踏まえ、どの開発言語に対応したSBOM ツールを導入する必要があるかを整理することが望まれる。

観点	説明
日本語対応	現状のところ、海外で開発された SBOM ツールがほとんどである。そのため、取扱説明書や README ファイルが英語のみで提供されているケースがあるほか、ツール自体も日本語対応していない場合がある。英語のみで提供されているツールの運用が困難である場合には、自組織の SBOM 導入の目的やその他の観点を踏まえて検討した上で[25]、日本語対応しているツールの優先度を高めることが考えられる。なお、有償ツールの販売代理店や無償ツールのサポートを提供している企業において、SBOM ツールに関するドキュメント類を日本語に翻訳して提供している場合もある。

SBOM 導入の目的や SBOM 適用範囲を踏まえ、各観点について、どの程度の内容を求めるか、予め整理した上で SBOM ツールを評価・選定することが望まれる。例えば、SBOM 導入に際して利用できる社内の予算が限定的である場合、無償の SBOM ツールから、自社の開発言語に対応し、所要のフォーマットで SBOM を出力できるツールを選定することが想定される。有償ツールを導入できる予算が充てられている場合、機能、性能、コスト等を総合的に勘案し、複数のツールを評価した上で、ツールを選定することが想定される。なお、事業部門や開発プロジェクトごとに求める最適なツールの観点が異なる場合等を除き、複数の SBOM ツールの使い分けが非効率となる場合があることに留意が必要である。

ツールの評価・選定に当たっては、SBOM ツールを扱う代理店に相談することも想定される。SBOM ツールの導入前に無償トライアル[26]等を利用して実際の使用感を体験し、操作学習の難易度及び必要期間を評価することで、自社における典型的な製品や適用を想定しているプロジェクトのソースコードを試験的に解析し、期待通りの結果が得られるかどうかを確認することができる。また、観点の設定や選定に難しさを感じる場合には、複数の SBOM ツールを扱う販売代理店に相談し、多くのツールに関する情報を把握しつつ、各ツールの特徴や長所・短所を比較評価しながら選定することも想定される。

4.3. SBOM ツールの導入・設定

【SBOM 導入に向けた実施事項】

□ SBOM ツールが導入可能な環境の要件を確認し、整備する。

□ ツールの取扱説明書や README ファイルを確認して、SBOM ツールの導入・設定を行う。

[25] 例えば、自社海外拠点、海外提携先、外資サプライヤー等と SBOM ツールを共同運用する可能性がある場合、日本語対応の優先度より、ツールの機能、性能、運用方法等を踏まえたツール選定が望まれる等、導入目的や他の観点も踏まえた検討が必要である。

[26] なお、トライアルを実施する前に評価したい機能やユースケースを整理し、具体的なトライアル計画を策定することが効果的である。

【SBOM 導入に向け認識しておくべきポイント】

- サポート体制が整備されている有償の SBOM ツールにおいては、販売代理店やツールベンダーに対して問合せを行い、支援を受けることで、効率的にツールの導入・設定を行うことができる。
- 無償の SBOM ツールでは、ツールの構築や設定に関する情報が不足している場合があるため、試行錯誤的に設定を行うための負担を強いられる可能性がある。必要に応じて、無償ツールに関するサポートサービスを提供している企業の支援を受けることで、効果的な無償 SBOM ツールの導入・設定が可能となる。
- SBOM ツールを脆弱性管理に活用する場合、障害等の影響で SBOM ツールが停止し、脆弱性の検知が滞ることのないよう、稼働監視やデータの定期的なバックアップを実施する必要がある。

SBOM ツールによって導入可能な環境が異なり、例えば、ツールが動作する PC について、インターネット接続があること、一定以上のマシンスペックを有すること、特定の OS であること、特定のブラウザをインストールしていること、Java や Python の実行環境が整っていること等が求められる場合がある。また、一部の SBOM ツールでは導入可能な OS が Linux に限定されており、Windows 端末にインストールする場合、別途仮想マシン環境が必要となる場合がある。そのため、SBOM ツールの導入・設定に当たっては、まず当該ツールの導入要件を確認し、導入できる環境を整備することが必要である。

導入できる環境が整備できた後、実際に SBOM ツールを導入し、SBOM 作成に向けた初期設定を行う。基本的には、取扱説明書や README ファイルを確認して導入・設定を行うこととなるが、サポート体制が整備されている有償の SBOM ツールにおいては、販売代理店やツールベンダーの支援を受けることで、効率的にツールの導入・設定を行うことができる。環境構築や初期設定の代行サービスを提供している販売代理店もあるため、必要に応じてそれらのサービスの活用を検討するのも一案である。特定の SBOM ツールでは、ツールの構築や設定に関する情報が不足している場合がある。また、多くの無償 SBOM ツールは海外で開発されているため、参考となるドキュメントが英語のみであることが多い。そのため、サンプルコードを入力して所望の SBOM が出力されるかを確認する等、試行錯誤的に設定を行うことも想定される。必要に応じて、無償ツールに関するサポートサービスを提供している企業の支援を受けることで、効果的な無償 SBOM ツールの導入・設定が可能となる。

なお、SBOM ツールを脆弱性管理に活用する場合、障害等の影響で SBOM ツールが停止し、脆弱性の検知が滞ることのないよう、稼働監視やデータの定期的なバックアップを実施する必要がある。

4.4. SBOM ツールに関する学習

【SBOM 導入に向けた実施事項】

□ ツールの取扱説明書や README ファイルを確認して、SBOM ツールの使い方を習得する。

□ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

【SBOM 導入に向け認識しておくべきポイント】

- サポート体制が整備されている有償の SBOM ツールにおいては、販売代理店やツールベンダーに対して問合せを行うことで、効率的にツールの使い方を習得することができる。
- サンプル SBOM の作成等を通じて試行錯誤的にツールを使うことで、効率的にツールの使い方を習得できる。

SBOM ツールが導入・設定できた後、当該ツールの使い方を習得することが望まれる。上記のツールの導入・設定と同様に、基本的には、取扱説明書や README ファイルを確認してツールの使い方を習得することとなるが、サポート体制が整備されている有償の SBOM ツールにおいては、販売代理店やツールベンダーに対して問合せを行うことで、効率的にツールの使い方を習得することができる。無償ツールと比較して有償ツールは高機能であるため、すべての機能に関する習得に時間がかかる可能性がある。自組織が作成したい SBOM 作成に必要な機能を販売代理店やツールベンダーに確認し、当該機能に絞って使い方を習得することも想定される。また、サンプル SBOM の作成等を通じて、試行錯誤的にツールの使い方を習得することも効果的である。特に、使い方に関する情報が不足しているツールの場合に効果的である。なお、ツールの具体的な使い方は組織によって異なるところ、学習プロセスを通じて明らかとなったツールの使い方に関するノウハウや各機能概要を記録し、組織内で共有することが望まれる。

5. SBOM 作成・共有フェーズにおける実施事項・認識しておくべきポイント

構築した環境や体制に基づき実際に SBOM を作成し、必要に応じて SBOM を提供することが求められる。本章では、SBOM 作成・共有フェーズにおいて SBOM 導入組織が実施すべき事項や、SBOM 導入組織が認識しておくべきポイントを示す。

5.1. コンポーネントの解析

【SBOM 導入に向けた実施事項】

□ SBOM ツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析する。

□ SBOM ツールの解析ログ等を調査し、エラー発生や情報不足による解析の中断や省略がなく、解析が正しく実行されたかを確認する。

□ コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れがないかを確認する。

【SBOM 導入に向け認識しておくべきポイント】

- SBOM ツールのコンポーネント解析機能を用いることで、手動の場合と比較し、効率的にコンポーネントの解析及び SBOM の作成を行うことができる。SBOM ツールを用いることの効果はコンポーネント数が多いほど大きい。
- パッケージマネージャーの構成情報を活用することが効果的な場合がある。また、パッケージマネージャーを用いることで、SBOM ツールのコンポーネント解析機能では特定できない粒度の細かいコンポーネントを特定できる場合がある。
- コンポーネントの誤検出や検出漏れが生じる場合がある。例えば、シンボリックリンクやランタイムライブラリ等のコンポーネント、深い階層のコンポーネント、特定分野でのみ利用されているコンポーネント等を検出できない場合があるほか、コンポーネントを特定できてもバージョン情報が誤っている場合がある。
- SBOM ツールにおけるコンポーネント解析方法によって、出力結果が異なる。依存関係に基づく解析の場合、誤検出の発生可能性は極めて低いが、その他の解析方法の場合、誤検出・検出漏れが発生する可能性がある。また、バイナリファイルに基づく解析の場合、ソースコードを利用できない場合でもバイナリファイルのみで解析可能というメリットがある一方で、バイナリファイルのみを用いた場合、解析精度が下がる可能性がある。
- コンポーネントを解析する環境（実行環境、開発環境等）によって、解析結果が異なる場合がある。

- SBOM ツールのデータベースに存在しない OSS は検出できないため、SBOM ツールのコンソールから手動でコンポーネントに関する情報を追加する等、追加対応が必要となる場合がある。
- SBOM ツールによって作成された SBOM におけるコンポーネントの関係性が、実際のソフトウェアの構成と異なる場合があるため、適切な設定を施した上で解析する必要がある。
- サブ階層のコンポーネントやサードパーティコンポーネントに関する誤検出や検出漏れの確認には特に大きな工数を要する。検出漏れの保証は困難であるため、正確性の度合いと対応工数とのトレードオフを踏まえた確認が必要となる。
- SBOM ツールの解析方式を考慮することで、効率的に誤検出や検出漏れを確認することができる。

実証を通じて、SBOM ツールのコンポーネント解析機能を用いることで、手動の場合と比較し、効率的にコンポーネントの解析及び SBOM の作成を行うことができることを確認した。例えば、医療機器分野の歯科用 CT を対象とした実証では、手動での SBOM 作成には 30 人時間以上の工数が必要になった一方で、SBOM ツールを用いた場合、0.15 人時間で SBOM 作成できることを確認でき、ツールを用いることで 99%以上の工数削減につながることを確認した。そのため、SBOM ツールを用いたコンポーネントの解析及び SBOM の作成・管理を行うことが現実的であり、本節でも SBOM ツールを前提とした記載を行う[27]。なお、パッケージマネージャーを用いることで、SBOM ツールでは特定できない粒度の細かいコンポーネントを特定できる場合があり、パッケージマネージャーの構成情報を活用することで、効果的に SBOM を作成できる場合がある。また、可能な場合に、ソフトウェアサプライヤーから SBOM を受領することで、効率的に SBOM を作成できる。

SBOM 作成に向け、まず、SBOM ツールのコンポーネント解析機能に基づいて対象ソフトウェアをスキャンし、コンポーネントの情報を解析する。SBOM ツールによってスキャン方法が異なり、GUI 上から対象ソフトウェアを指定して解析する場合もあれば、CLI にて解析を行う場合もあるため、解析の方法について、導入した SBOM ツールの取扱説明書や README ファイルを確認する。解析を行うことで、対象ソフトウェアに含まれるコンポーネントの名称、サプライヤー名、バージョン、コンポーネント間の依存関係等を洗い出すことができる。ただし、コンポーネントの誤検出や検出漏れが生じる場合があることに留意する必要がある。事実、実証において、以下の点が明らかとなった。

- シンボリックリンクやランタイムライブラリ等、実体が SBOM ツールのスキャン対象に含まれないコン

[27] その他の SBOM 作成方法として、ソフトウェアのビルド時に SBOM を自動生成する方法も存在する。例えば、以下のようなビルド環境・ツール利用による SBOM 生成例が公開されている。

- Yocto での SBOM 作成方法：https://docs.yoctoproject.org/dev/dev-manual/sbom.html
- Android Open Source Project（AOSP）での SBOM 作成方法：https://source.android.com/docs/setup/create/create-sbom?hl=ja
- Zephyr での SBOM 作成方法：https://docs.zephyrproject.org/latest/develop/west/zephyr-cmds.html

ポーネントが検出されなかった。

- 最上位のコンポーネントの検出結果と比較して、下位のコンポーネントに関する検出漏れ率が高かった。ただし、最上位のコンポーネントが検出されずに下位のコンポーネントのみが検出されるケースもあり、必ずしもコンポーネントの階層で検出率が変わるわけではないことが分かった。
- 特定分野でのみ利用されている制御に関するコンポーネントが検出されなかった。
- バージョン情報が誤って検出されたコンポーネントが複数存在した。
- SBOM ツールにおけるコンポーネント解析方法によって、出力結果が異なった。バイナリファイルのみを用いたバイナリスキャンの結果について、通常スキャンで検出されたコンポーネント数と比較して 1 割程度しか検出されなかった。
- コンポーネントを解析する環境によって、解析結果が異なった。開発環境でスキャンを行った場合、実際に製品には使用されないアンインストールパッケージも検出された。
- SBOM ツールのデータベースに存在しない OSS は検出できず、SBOM ツールのコンソールから手動でコンポーネントに関する情報を追加する等、解析結果の調整が必要となった。
- SBOM ツールのリポジトリや設定により、SBOM 中のコンポーネントの構成情報が異なり、SBOM ツールによって作成された SBOM におけるコンポーネントの関係性が、実際のソフトウェアの構成と異なるケースがあった。
- SBOM ツールで検出されたコンポーネントとパッケージマネージャーで抽出したコンポーネントが一致しないケースがあった。

よって、SBOM ツールのコンポーネント解析機能の出力結果をそのまま用いるのではなく、誤検出や検出漏れに関して出力結果を確認することが重要である。結果に対する誤検出や検出漏れの確認の観点及び確認方法は図 5-1 に示すとおりである。なお、誤検出や検出漏れの確認は基本的に人手で実施する必要があるため、網羅的に確認することが現実的に難しい場合がある。実証では、誤検出や検出漏れの確認に 0.50 人時間を要したコンポーネントも存在し、コンポーネントが膨大なソフトウェアの場合、誤検出や検出漏れの確認に関して多大な工数が必要となる。特に、サブ階層のコンポーネントやサードパーティコンポーネントに関する誤検出や検出漏れの確認には大きな工数を要する。検出漏れの保証は困難であるため、正確性の度合いと対応工数とのトレードオフを踏まえた確認が必要となる。

確認の観点		確認方法
ツールが正しく動作しているか		① ツールの実行ログにエラーが無いかを確認する。
コンポーネントの解析結果が正しいか	コンポーネントを誤検出していないか	② 出力されたコンポーネントが、対象ソフトウェアに含まれているかを確認する。マッチタイプが完全一致でない場合、コンポーネントが改変されている可能性が無いかを確認する。 ③ （②で判断がつかない場合）出力されたコンポーネント名を元に、GitHub等の外部ソースから入手したソースコードと対象ソフトウェアのソースコードとを比較する。
	使用しているコンポーネントが含まれているか（検出漏れが無いか）	④ 対象ソフトウェアに含まれるコンポーネントが出力結果に含まれているかを確認する。
	改変されたコンポーネントを検出できているか	⑤ スニペット解析の結果をもとに、対象ソフトウェアのソースコードと元のソースコードとを比較する。
	検出できていないコンポーネントが無いか	⑥ 対象ソフトウェアのCopyrightを抽出し、検出したコンポーネントが出力結果に含まれているかを確認する。

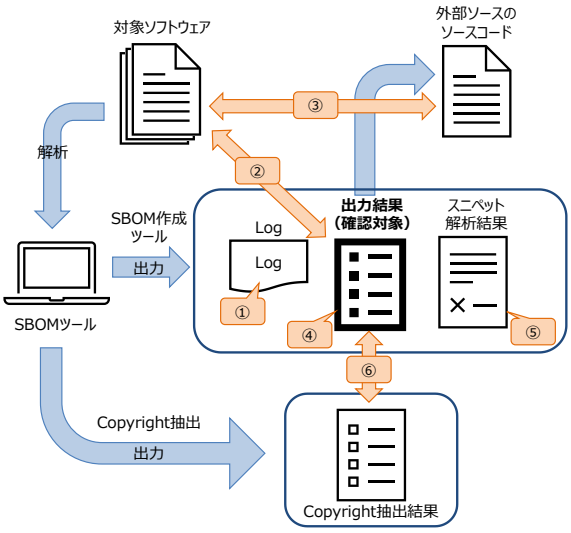

図 5-1 コンポーネント解析結果の確認の観点及び確認方法

誤検出や検出漏れの確認に当たっては、SBOM ツールの解析方式を考慮することが重要である。ツールにおけるコンポーネントの解析方法には、コードマッチング、依存関係検出、文字列検出の大きく 3 つの方法が存在する。依存関係検出は、パッケージマネージャーで取得する直接的・間接的な OSS を検出する方法であり、誤検出の発生可能性は低い。一方で、コードマッチングや文字列検出による解析の場合、誤検出や検出漏れが発生する可能性がある。また、バイナリファイルに基づくスキャンの場合、多くの検出漏れが発生したことが実証で明らかとなった。コンポーネントの解析方式によって誤検出や検出漏れの発生度合いが異なるところ、使っている SBOM ツールの解析方式を踏まえた誤検出や検出漏れの確認が望まれる。例えば、バイナリファイルに基づく解析の場合、ソースコードを利用できない場合でもバイナリファイルのみで解析可能というメリットがある一方で、バイナリファイルのみを用いた場合、誤検出や検出漏れが多数発生する可能性があるということ等も踏まえながら、誤検出や検出漏れを確認することが想定される。また、SBOM ツールのパラメータ設定の不足や、パッケージマネージャーの実行失敗等の理由により解析が正常に実施できておらず、誤検知や検出漏れが発生している可能性もある。表面上は正常終了しているように見えても、エラーにより内部的な解析プロセスの一部をスキップして終了している場合もあるため、ツールの実行ログを確認し、そのようなエラーが発生していないかを確認する必要がある。

誤検出や検出漏れの確認の結果、未知の情報や不明の情報が含まれていることが分かった場合、その情報を「既知の未知」として把握することが望まれる。「既知の未知」とは、不明ではあるものの、不明である事実を既知としておくことであり、表 2-3 で記載のとおり、SBOM の「最小要素」においても言及されている。作成した SBOM を対象ソフトウェアの利用者や納入先に共有する場合、「既知の未知」な情報も合わせて共有することで、情報の透明性を高めることができる。

5.2. SBOM の作成

【SBOM 導入に向けた実施事項】

□ 作成する SBOM の項目、フォーマット、出力ファイル形式等の SBOM に関する要件を決定する。

□ SBOM ツールを用いて、当該要件を満足する SBOM を作成する。

【SBOM 導入に向け認識しておくべきポイント】

- SBOM 作成と共有の目的を鑑み、正確な情報を不足なく SBOM に記載することが望ましい。
- サードパーティや OSS コミュニティ等の第三者から提供されたコンポーネントを使用している場合は、当該コンポーネントの SBOM の提供を受けることができる場合もある。ただし、そのコンポーネントを自組織にて改変して使用している場合は、提供を受けた SBOM をそのまま利用できなくなるので注意が必要である。
- SBOM 内の名称について、SBOM 利用者の視点で名称設定を行うことで、SBOM 共有後の手戻りをなくすことができる。

解析したコンポーネントの情報に基づき、SBOM を作成する。SBOM の作成に当たっては、SBOM に含める項目、フォーマット、出力ファイル形式等の SBOM に関する要件を事前に決定する必要がある。これらの要件について、規制・要求事項において、SBOM のフォーマットや項目が定められている場合がある。SBOM のフォーマットでは、情報なし（NOASSERTION）も許容されるが、SBOM 作成と共有の目的を鑑み、正確な情報を不足なく SBOM に記載することが望まれる。なお、サードパーティや OSS コミュニティ等の第三者から提供されたコンポーネントを使用している場合は、当該コンポーネントの SBOM の提供を受けることができる場合もある。第三者から SBOM の提供を受けることで、効率的に SBOM が作成できるほか、自社で作成した SBOM の精査に当たって活用することも想定される。ただし、コミュニティや個人に対して SBOM の提供を依頼すべきか否かについては、契約やライセンスの問題があることに注意が必要である。また、サプライチェーン上でのコンポーネントの書換えや不正改ざんを把握するためには、第三者から提供された SBOM と自組織で作成した SBOM を突合し、整合性を確認することが効果的である。加えて、SBOM の共有先となりうるソフトウェアの利用者及びサプライヤーから指定される場合もあるため、自社の状況を鑑み、SBOM の要件を決定することが必要となる。具体的な SBOM 作成方法はツールによって異なるため、導入した SBOM ツールの取扱説明書や README ファイルを確認する必要がある。

SBOM は作成するだけでなく継続的に管理することが求められるところ、SBOM の作成日時は明確に記録することが求められる。また、ソフトウェアサプライチェーンの透明性を高めるために、必要に応じて作成した SBOM を対象ソフトウェアの利用者や納入先に共有することが望まれるが、共有に際して、作

成した SBOM のフォーマットが有効であり、必要な情報が含まれているか、確認することが求められる。

作成された SBOM には、コンポーネントの情報だけでなく、プロジェクト名称等のツール上で設定した情報も含まれる場合がある。この情報について、SBOM 利用者が活用しやすい情報となっているかを検討することが望まれる。開発段階から SBOM ツールの管理機能を用いてコンポーネントを管理する場合、そこで使用しているプロジェクト名称やバージョン情報が SBOM に反映されるため、これまで社内のみで使われていた情報が SBOM 利用者に共有される可能性がある。SBOM 内の名称について、SBOM 利用者も理解できる名称設定を行うことで、SBOM 共有後の手戻りをなくすことができる。

5.3. SBOM の共有

【SBOM 導入に向けた実施事項】

□ 対象ソフトウェアの利用者及び納入先に対する SBOM の共有方法を検討した上で、必要に応じて、SBOM を共有する。

□ SBOM の共有に当たって、SBOM データの改ざん防止のための電子署名技術等の活用を検討する。

【SBOM 導入に向け認識しておくべきポイント】

- 納入先が利用する SBOM ツールによって、採用可能な SBOM 共有方法が異なる。
- 利用者に対する SBOM 共有について、様々な方法が想定される。利用者に対して SBOM 共有を行う場合、それぞれの方法の長所短所を踏まえて検討する。

ソフトウェアサプライチェーンの透明性を高める観点で、必要に応じて、ソフトウェアの利用者や納入先に対して作成した SBOM を共有することが望まれる。規制・要求事項として SBOM の共有が求められている場合には、当該事項で規定された内容に則り、適切な対象者に対して、適切な方法で SBOM を共有することが必要となる。共有方法の検討に際して、多くの SBOM は、コンポーネントのバージョンアップ等により作成後も動的に内容が変わることに留意する必要がある。なお、2.5 で記載のとおり、SBOM の公開は必須ではなく、SBOM 作成者やサプライヤーの判断で SBOM の共有方法を判断することが望まれる。

納入先に SBOM を共有する場合、納入先が利用する SBOM ツールによって共有の方法が異なる。一般的に、自組織と納入先とが同じ SBOM ツールを利用している場合、SBOM の共有は比較的容易に実施することができ、特に有償の SBOM ツールの場合、自組織と利用者・納入先とがクラウド上で同一の SBOM ツールを使用することにより、SBOM を共有できるケースもある。一方、自組織と利用者・納入先とが異なる SBOM ツールを用いている場合、ツールによってインポートできる SBOM 形式や

フォーマットに制約がある場合があり、事前に納入先と、SBOM 共有方法や共有する SBOM の内容について協議することが望まれる。現状では、ほかのツールで生成した SBOM をインポートして脆弱性管理等に活用することができるツールは限られているため、利用者・納入先との間の協議の際には注意が必要である。

利用者に対する SBOM 共有について、様々な方法が想定される。例えば、製品内から SBOM を確認できるよう製品に組み込む方法、利用者がアクセス可能なリポジトリにおいて公開する方法、Web ページ上で公開する方法、共通の SBOM ツールを用いて SBOM データを共有する方法等が想定される。利用者に対する SBOM 共有を行う場合、SBOM 対象ソフトウェアの特性や更新の頻度、利用者における SBOM 利用状況等を踏まえ、どの方法で共有するかを検討することが望まれる。なお、SBOM 共有時の SBOM データ自体の信頼性を確保する目的で、改ざん防止のための電子署名技術や分散型台帳技術等の活用を検討することが求められる。

6. SBOM 運用・管理フェーズにおける実施事項・認識しておくべきポイント

SBOM のメリットを享受するために、作成した SBOM を運用・管理することが求められる。本章では、SBOM 運用・管理フェーズにおいて SBOM 導入組織が実施すべき事項や、SBOM 導入組織が認識しておくべきポイントを示す。

6.1. SBOM に基づく脆弱性管理、ライセンス管理等の実施

【SBOM 導入に向けた実施事項】

□ 脆弱性に関する SBOM ツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。

□ ライセンスに関する SBOM ツールの出力結果を踏まえ、OSS のライセンス違反が発生していないかを確認する。

【SBOM 導入に向け認識しておくべきポイント】

- SBOM ツールが出力した脆弱性情報やライセンスに関する情報が誤っている場合があり、出力結果を確認する必要がある。
- SBOM ツールでコンポーネントの EOL を特定できない場合、別途個別に調査する必要がある。

SBOM 運用・管理フェーズでは、作成された SBOM に基づき、脆弱性管理やライセンス管理等を行う。前述のとおり、SBOM はソフトウェア管理の一手法であるため、SBOM を作成すること自体を目的とせず、SBOM を活用しつつ、適切なソフトウェア管理を目指すことが重要となる。よって、第三者から提供された SBOM データに対しても、脆弱性管理やライセンス管理等、同様の対応を実施することが求められる。脆弱性管理に当たっては、SBOM ツールの脆弱性管理機能の出力結果を踏まえ、ソフトウェアに含まれるコンポーネントの脆弱性有無を確認するとともに、脆弱性が確認された場合には、当該脆弱性に対する対応を実施することが必要となる。具体的な脆弱性対応として、脆弱性の箇所を特定し、影響範囲を分析するとともに、リスクの推定及び評価を行い、リスクの受容可能性を確認し、脆弱性対応の優先付けを行うことが望まれる。そして、関連するセキュリティ問題の特定を行った上で、脆弱性の深刻度を評価し、緊急性の判断を行うことが望まれる。自社のプロプライエタリソフトウェアで脆弱性が確認された場合、関連するソフトウェア利用者に対して適切に通知するほか、OSS や汎用ソフトウェア等のサードパーティコンポーネントで脆弱性が確認された場合、当該コンポーネントのサプライヤーに対して脆弱性を通知することが望まれる。なお、脆弱性の影響範囲分析においては、ソースコードのみならず、要件定義書、仕様書、テスト仕様書等の開発文書の更新必要範囲の特定・分析も必要であることに留

意すべきである。この点の対策例として、2021 年度の実証では、SBOM ツールと既存の構成管理ツールを連携させることで、脆弱性の影響範囲特定の工数削減につながる可能性が確認された。

手動で SBOM を管理する場合、一つ一つの脆弱性の有無を手作業で特定するほか、個別に脆弱性を評価し、さらに対応方針を個々に検討する必要がある。脆弱性の情報が日々更新されることを踏まえると、手動での SBOM 運用・管理は非現実的である。よって、図 6-1 に示すとおり、脆弱性管理においても、SBOM ツールを用いた管理が想定される。有償・無償の SBOM ツールにより、脆弱性マッチングの範囲に差が大きいことに留意が必要である。無償ツールには脆弱性マッチングの機能がないものもあり、有償ツールでは、NVD、JVN のような公的な脆弱性情報データベース以外に、独自に脆弱性情報データベースを強化し、脆弱性マッチングの範囲を拡大したものがある。有償の SBOM ツールによっては、解析されたコンポーネントと脆弱性情報を自動でマッチングし、その脆弱性の深刻度やリスク、対処方法等を提示するため、脆弱性の発見から深刻度評価、対処方法の特定までを非常に迅速に行うことができるツールも存在する。ただし、脆弱性情報が特定されたとしても具体的な対処方法までは提示されない場合は、個々の脆弱性の内容を踏まえて対処方法を別途検討する必要がある。

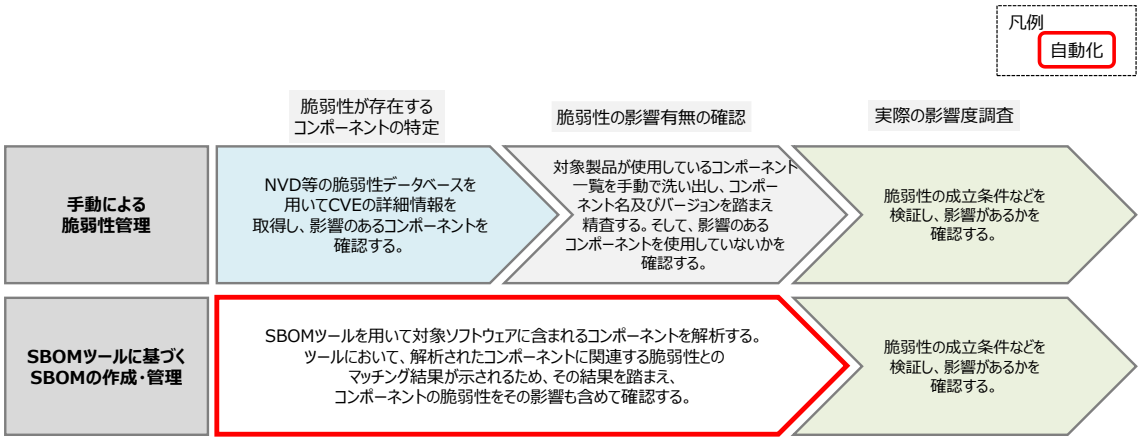

図 6-1 手動と SBOM ツールでの脆弱性管理手順の比較

SBOM ツールに基づく脆弱性管理に当たって認識しておくべきポイントとして、SBOM ツールが出力した脆弱性情報に誤りがあることが挙げられる。実証において利用した無償の SBOM ツールにおいて、脆弱性の深刻度が誤って出力されたケースがあり、手動で脆弱性情報を調査することが必要となった。コンポーネントの解析に当たって誤検出や検出漏れが生じる可能性があるところ、脆弱性情報の出力結果においても誤りが生じる可能性もあり、出力結果を確認することが必要となる。SBOM ツールによっては、NVD といった公開脆弱性情報データベースに掲載されている脆弱性情報だけでなく、ツールベンダー独自の調査に基づく脆弱性情報を活用して脆弱性のマッチングを行うツールもあり、幅広い脆弱性の情報に基づく脆弱性管理が可能となる場合がある。

このような観点や課題に対応して、7 章においては、SBOM を用いた脆弱性管理について具体的な手順や手法に関してプロセスのフェーズに分けてまとめている。

ライセンス管理も同様である。SBOM ツールの出力結果を踏まえ、ソフトウェアに含まれるコンポーネン

トのライセンスコンプライアンスの状況を確認するとともに、当該コンポーネントの想定利用方法に対して遵守不可能又は遵守困難なライセンス条件が確認された場合には、利用コンポーネント自体の変更や利用方法の変更等、対応を実施することが必要となる。脆弱性管理と同様に、手動での管理ではなくSBOM ツールでの管理が現実的である。

SBOM ツールを用いることで、対象ソフトウェアに含まれるコンポーネントにおける脆弱性やライセンスの情報を効率的に特定できる一方で、ツールを用いてコンポーネントの EOL を特定することは一般に難しく、手作業で特定することが必要となる。EOL に関する情報がないコンポーネントも存在するところ、可能な限りこのようなコンポーネントを使用しない等を設計時に考慮することが望まれる。

6.2. SBOM 情報の管理

【SBOM 導入に向けた実施事項】

□ 作成した SBOM は、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する。

□ SBOM に含まれる情報や SBOM 自体を適切に管理する。

【SBOM 導入に向け認識しておくべきポイント】

- 自動で脆弱性情報が更新・通知される SBOM ツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置する等運用面でカバーする必要があるが、対応工数を要する。
- SBOM の管理は、組織内の PSIRT に相当する部門が対応することが効果的である。PSIRT に相当する部門が存在しない場合、品質管理部門にて対応することが効果的である。

作成した SBOM は、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する。保管期間は、一般的に対象製品が市場に流通している間や対象サービスが提供されている期間は最低限としつつ、販売終了後も、保証期間、サポート提供期間、交換部品の提供期間等に必要に応じて SBOM を参照する可能性があるため、予め参照できるように準備しておく必要がある。さらに、使用しているコンポーネントのライセンスの条件で製品提供終了後 3 年等の個別の指定がある場合にはその期間も考慮する必要がある。また、出荷済み製品と SBOM 情報とを対応づけられるよう、SBOM の改変履歴も含めて資産管理システム等で保管することも想定される。

SBOM の対象としたソフトウェアの内容が動的に変わるほか、脆弱性の情報も日々更新されることを踏まえ、SBOM に含まれる情報は定期的に更新し、管理する必要がある。自動で脆弱性情報が更新・通知される SBOM ツールを用いることで、新たな脆弱性に関する情報を即座に把握することができ

る。ツールを用いた自動管理ができない場合、担当者を別途設置する等運用面でカバーすることとなるが、ツールでの管理と比較して対応工数を要することに留意が必要である。

SBOM の管理体制について、脆弱性管理という観点を踏まえると、組織内の PSIRT 又はそれに類する部門が主導して SBOM の管理を行うのが望ましい。また、作成された SBOM を PSIRT が活用することで、実際に利用者の環境で用いられている OSS の絞り込みに必要な工数が削減され、より効率的な脆弱性対応や監視が可能になる。PSIRT に相当する部門が存在しない場合でも、脆弱性管理は一定のポリシーの下で実施されることが必要であり、例えば、品質管理部門にて SBOM を管理することが望まれる。会社横断で品質管理を担うチームが存在するようであれば、品質管理の一貫として、成果物としての SBOM の定義や管理、SBOM 活用による脆弱性の対応を行うことで、一定のポリシーの下での運用が可能になる。もし、品質管理部門も存在しない場合、まずは特定の製品開発チームで SBOM ツールを導入し、SBOM の作成から運用・管理に至るノウハウを蓄積することから始めることが期待される。その後、得られたノウハウを別の開発チームに横展開し、チームごとで SBOM 導入を進めることで、社内の SBOM 導入レベルを向上することが望まれる。

7. 脆弱性管理プロセスの具体化

7.1. 目的

SBOM の活用によるセキュリティ面における効果として、脆弱性管理により、脆弱性を特定し、対応することで悪用される可能性の低減を挙げることができる。したがって、SBOM の作成、共有、運用、管理の全体のプロセスのうち、脆弱性管理に関わるフェーズが特に重要といえる。本章では、SBOM を用いた脆弱性管理プロセスにフォーカスして具体的な手順と考え方についてまとめることで、SBOM の効果を高める参考情報を提供する。

7.2. 脆弱性管理における課題・問題認識

SBOM を活用した脆弱性管理の効率化・普及促進においては、機器メーカー、部品サプライヤー、ユーザー組織など様々なステークホルダーが関係し、脆弱性管理プロセスにおける、技術、標準、手順などに関して様々な課題が存在する。下図は、脆弱性管理プロセスを横軸として主な課題について全体像を示したものである。

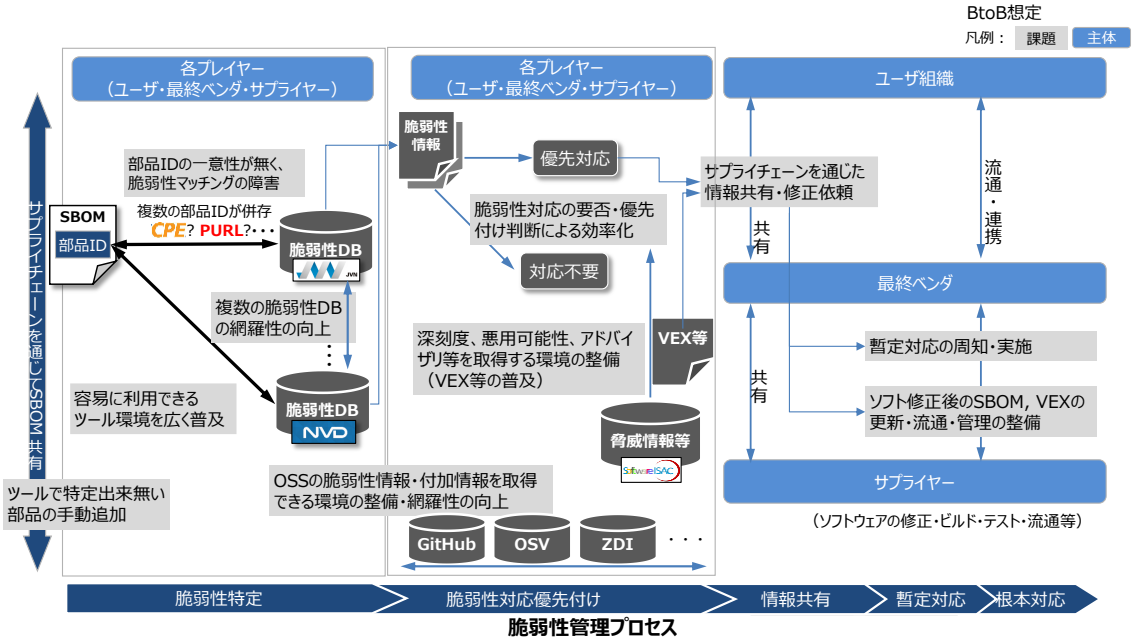

図 7-1 SBOM を活用した脆弱性管理における課題（全体像）

SBOM を活用した脆弱性管理プロセスは、図の横軸に示すとおり、脆弱性特定、脆弱性対応優先付け、情報共有、脆弱性対応（暫定対応、根本対応）のフェーズとして実施することができる。SBOM を活用した脆弱性管理には、課題が存在するため、これらのフェーズにおける課題を示し、それらの課題を解決するための方法・手順を次節で示す。

まず、脆弱性特定フェーズにおいては、SBOM に含まれる部品 ID に様々な標準、ベンダー独自形式があり一意性がないため脆弱性マッチングの障害となることが挙げられる。また、脆弱性 DB は複数存

在し、脆弱性情報の網羅性を高めるには対象とする脆弱性 DB の範囲の拡大が課題となる。脆弱性対応優先付けフェーズにおいては、脆弱性対応の効率化のため、対応要否の判定、優先付けが課題となる。その際に必要となる情報について外部からの取得や VEX（Vulnerability Exploitability Exchange）情報の普及が課題となる。情報共有フェーズにおいては、情報共有の範囲の特定や手段、環境の整備が課題となる。脆弱性対応フェーズにおいては、脆弱性の修正を伴わない暫定対応策の検討や、脆弱性修正の結果に伴う SBOM、VEX 情報の更新や共有が課題となる。

以下の章では、このような課題を解決するための方法や手順を示すことで、SBOM を活用した脆弱性管理を実現するための方法を示す。

7.3. プロセス全体像

前節の課題を踏まえて、SBOM を用いた脆弱性管理を実施する上で重要になる方法と手順の全体像を整理すると以下のようになる。

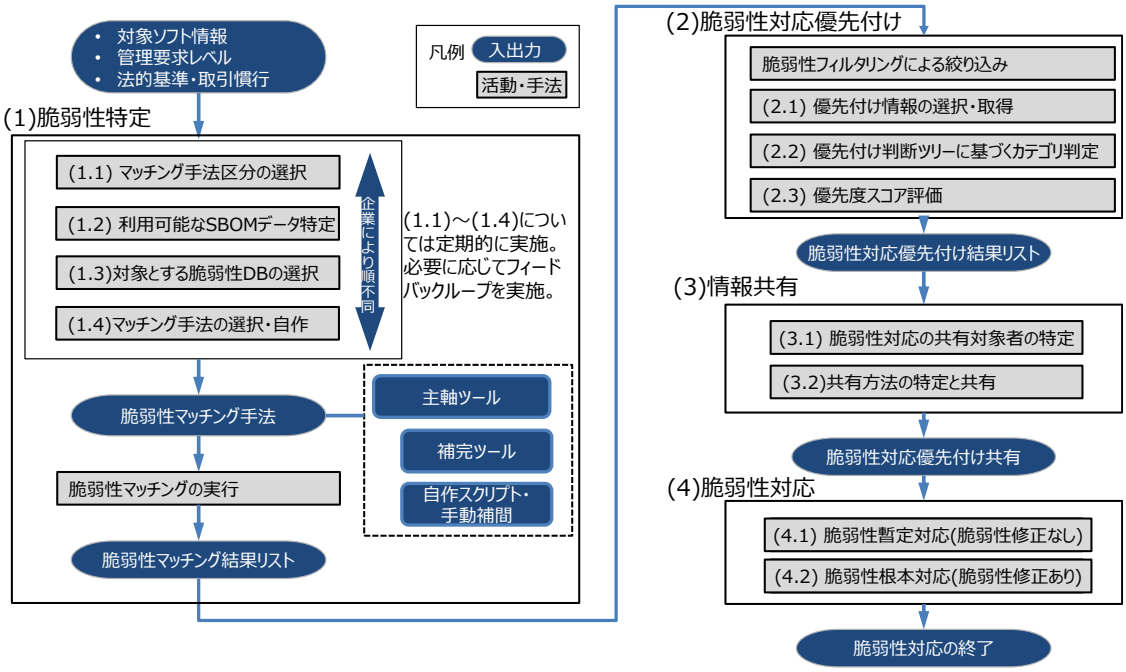

図 7-2 SBOM を活用した脆弱性管理プロセスの重要ステップと手順（全体像）[28]

図に示すとおり、SBOM を用いた脆弱性管理プロセスは以下の４つのステップから構成される。本節では、各ステップについて、重要な方法と手順について参考例を示す。

---

[28] 脆弱性管理プロセスについては、以下のような文書などを参考に整理した。
NTIA, “Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)”,
CISA, “Stakeholder-Specific Vulnerability Categorization (SSVC)”,
CISA, “SBOM Sharing Roles and Considerations”

(1) 脆弱性特定フェーズ
対象ソフトウェアに対して、SBOM を用いて最新の脆弱性情報から、ソフトウェアに含まれる脆弱性を特定する。
(2) 脆弱性対応優先付けフェーズ
特定された脆弱性情報について、悪用可能性や費用対効果の関係から対応の要否、優先度付けを行う。
(3) 情報共有フェーズ
脆弱性情報、対応方法などについて、ステークホルダー間での情報共有を行う。
(4) 脆弱性対応フェーズ
優先付けされた脆弱性に対して、脆弱性修正を含まない迅速な暫定対応と、脆弱性修正を含む根本対応を行い、その結果に伴い SBOM、 VEX 情報の更新、共有を行う。

7.4. 各フェーズの手順と方法

本章では、前章で示した SBOM を活用した脆弱性管理の各フェーズについて、具体的な手順や方法を示すことにより、各組織のポリシーや環境に応じて脆弱性管理を実現するため参考となる例を示す。

7.4.1. 脆弱性特定フェーズ

脆弱性特定は、主に、以下の４つの方法により組織ごとに脆弱性特定の手法を決定し、その手法を用いて実際の脆弱性特定を行う。これらの手法は、組織に応じて必要な項目や順序が異なるため、組織ごとに選択的に実施することが想定される。

脆弱性特定フェーズの実施方法

(1) マッチング手法区分の選択
脆弱性マッチング手法は、主に①SBOM 既存ツールの利用、②API 利用スクリプト、③WebUI に分けられ、組織の技術力、投入する費用・リソースに応じて選択する。
(2) 利用可能な SBOM データ特定
利用する SBOM の取得方法を特定する。
(3) 対象とする脆弱性 DB の選択
脆弱性特定や脆弱性対応優先付けにおいて利用する脆弱性 DB を選択する。
(4) マッチング手法の選択・実施
方法(1)から(3)の結果に基づき自組織の脆弱性特定手法を決定する。

(1)　マッチング手法区分の選択

脆弱性マッチング手法は下図に示すとおり、クライアント・サイドと脆弱性 DB サイドの構成に応じて、①SBOM 既存ツール、②API 利用スクリプト、③WebUI の三通りに分けられる。

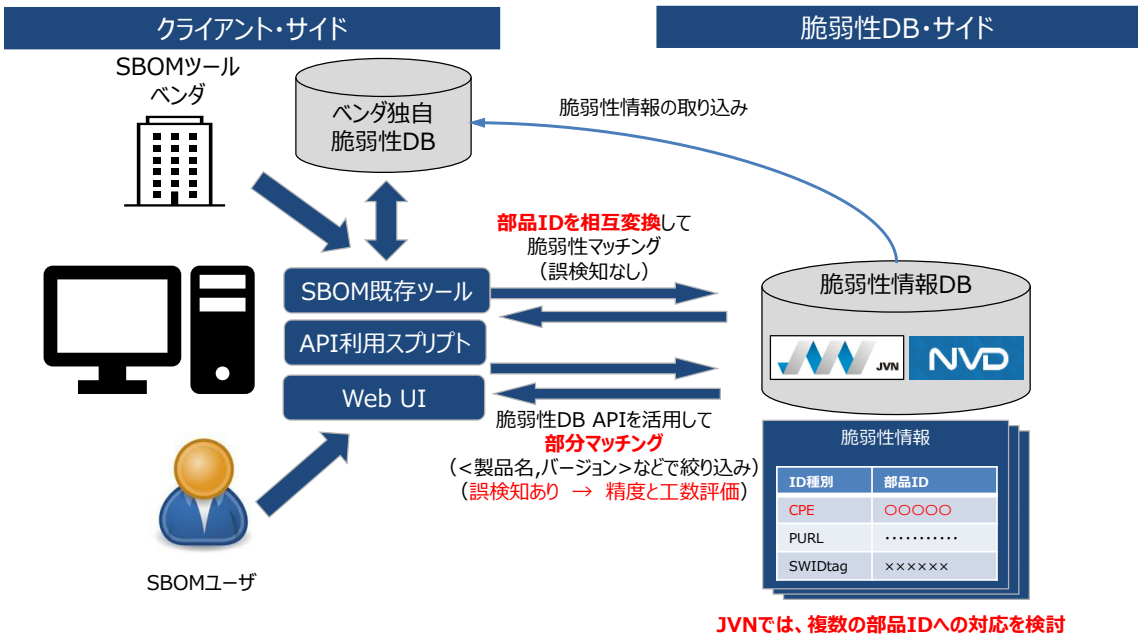

図 7-3 脆弱性マッチング区分の全体像と選択肢

これらの脆弱性マッチング区分について、ユースケース、主なユーザー、メリット・デメリットについて整理すると以下のようになる。これらも参考に各組織・ユーザーの状況において手法を選択することが想定される。

表 7-1 脆弱性マッチング区分のユースケース、主なユーザー、メリット・デメリットの整理

マッチング区分	ユースケース・必要性	主なユーザー	メリット・デメリット
API[29]の利用	既存ツールでは検索できない脆弱性 DB に対して、API を用いて脆弱性検索が可能となり、脆弱性検出の網羅性を高めることが	ソフトウェアに対する高い要求レベル（脆弱性リスクが低い）が求められるソフトウェアベンダー（メーカー、サプライヤー）が主なユーザーと想定される。また、重要インフラ事業者など要求レベルの高いユーザー企業についても、自律的に API を用いた網羅性の高い脆弱性検索が求められ	（メリット）API を利用して部品 ID の変換や脆弱性 DB の範囲拡大など柔軟にカスタマイズして、常時自動監視を行うことができる。検出漏れや誤検出などを防止する検索手法の作りこみ、検索後のアラート連動など可能になる。 （デメリット）API を用いたコーディングの技術力と工数等

[29] 脆弱性 DB が提供する API を指す。例えば、公的な例としては、MyJVN が提供する API などがある。

マッチング区分	ユースケース・必要性	主なユーザー	メリット・デメリット
	できる。	るケースがある。	のリソースが求められる。
既存ツールの利用	限られた人員、技術などのリソースの元で、既存ツールで検索可能な脆弱性 DB に限定して、最小限対応すべき脆弱性に対応する。	有償ツールの場合、予算に余裕のある大企業。無償ツールは、中小のユーザー組織、ベンダーなどの場合、API コーディングを行う人員、技術などが限られる組織。	（メリット）API コーディングなしに、限られた人員で脆弱性を特定できる。 （デメリット）既存ツールが提供される DB に対象が限定され、特定される脆弱性の網羅性が限定的になる。
Web UI 利用	API を用いたコーディングの前に、工数を抑えて、試行的に脆弱性の検索方法の検討や脆弱性の状況を確認する。	高度なセキュリティレベルを求められる API 利用者や、既存ツールの利用者が、定常業務前の試行的な脆弱性検索に利用する。	（メリット）API コーディングや既存ツールの利用による定常業務化前に、脆弱性検索の試行検討や脆弱性状況の把握ができる。 （デメリット）WebUI の利用は、手動操作が必要となるため、定常業務化できる API や既存ツールの利用よりも非効率となる。

(2)　利用可能な SBOM データ特定

利用可能な SBOM データは以下の考え方を参考に特定することができる。

① 対象ソフトウェアについてSBOMを外部から取得

- **サードパーティソフトウェアのSBOM提供状況の確認**
  OSSや既存のサードパーティソフトウェアについては、提供されるSBOMが予め決まっており、契約により必要なSBOMフォーマットを要求することが難しいため、事前に確認することが必要である。
- **委託開発契約におけるSBOMの規定**
  開発委託ソフトウェアについては、開発者の技術力、体制に応じて契約書などによりSBOMフォーマット、部品ID標準について合意を取ることが必要になる。

②ツールを用いたSBOMを生成

利用するソフトウェア（部品）について、ベンダー（サプライヤー）から取得することができない場合、SBOMツールを用いた自動生成、または、パッケージマネージャの構成情報等を利用したSBOM作成が必要となる。

図 7-4 利用可能な SBOM データの特定

なお、サードパーティソフトウェアについて、サプライヤーにより脆弱性管理が十分に保証されている場合は、調達者による脆弱性管理のための SBOM 取得の優先度が低くなる可能性がある。しかし、サプライヤーが企業として存続する保証はないため、サプライヤーに頼らず脆弱性管理を行うために、SBOM の取得が期待される。また、脆弱性管理以外の SBOM 活用法であるライセンス管理や構成管理等を行うためには、SBOM を取得することが必要となる。

SBOM フォーマットは代表的ものとして以下のものが候補となる。

SBOM フォーマット	開発主体	特徴
SPDX	Linux Foundation	知財・ライセンス管理を主目的に標準化。パッケージ、コンテナ、スニペットなどの対象を管理できる。
CycloneDX	OWASP	セキュリティ管理を主目的に策定。VEX を包含することが可能。
SWID	ISO/IEC, NIST	ソフトウェア ID 体系を含むソフトウェア管理の標準。

部品 ID 標準は、代表的なものとして以下のものが候補となる。

部品 ID	開発主体	特徴
PURL	OSS コミュニティ (gitter)	OSS など、パッケージマネージャーを中心にリポジトリに応じて ID が決定される分散割当方式である。
CPE	NIST	セキュリティ情報共有標準 SCAP の要素として規定。主に脆弱性が報告された際に CPE が割り当てられる。
SWID	ISO/IEC, NIST	CPE の上位互換で、NVD において CPE から SWID に移行を宣言しているが、現時点で採用は進んでいない。

なお、利用しようとしている SBOM が、対象ソフトウェアのどのタイミングを反映したものかを確認することが推奨される。SBOM は主に、ソースコード作成時、コンパイル時、ランタイム時などの作成タイミングによって、部品の網羅性などの違いがある[30]。SBOM データを取得する際は、脆弱性対応の対象システム・ソフトウェアの性質を踏まえ、どの作成タイミングの SBOM データが必要かを定義することが推奨される。また、実際に取得できた SBOM データがどのタイミングで作成されたかを確認の上、正確な脆弱性対応のために必要な作業を適宜調整することが推奨される。また、利用しようとしている SBOM が対象のソフトウェアのバージョンに適用可能なことを確認することが推奨される。異なるバージョンに対する SBOM を利用した場合、脆弱性マッチング対象のバージョンに含まれる SW 部品が正しく反映されておらず、脆弱性マッチングでの誤検知・検知漏れが発生するおそれがある。

(3) 対象とする脆弱性 DB の選択

脆弱性 DB の選択は、リスク低減、コスト低減の観点から比較を行い、個社ごとに優先度ポリシーを

[30] CISA, "Types of Software Bill of Materials (SBOM) Documents"

考慮して判断することが期待される。脆弱性 DB の選択は、脆弱性情報のカバレッジ拡大、脆弱性対応の迅速化、コスト効率化の観点から判断することが期待される。これらの観点の優先度は、個社によってポリシーが異なるため、個社・製品ごとに脆弱性 DB の対象範囲を選択することが期待される。例えば、コスト制約の強い中小企業は、費用、簡易ツールの利用を優先して DB を選択し、リスク低減の要求が高い企業は、カバレッジ拡大や対応の迅速化に対応した DB を優先的に選択する。

個社で優先度ポリシーを検討

比較優先事項			評価上位の脆弱性DB			基準例
リスク低減	脆弱性情報のカバレッジ拡大	脆弱性件数	民間DB 1	公的DB1	公的DB 2	件数カバー率7割以上
		CVE以外の脆弱性	民間DB2	民間DB3	民間DB4	CVE以外対象
		日本製品重点化	公的DB 2	—	—	日本製最大集合
		OSS重点化	民間DB4	民間DB2	民間DB5	重点化明示
リスク低減 / コスト低減	脆弱性対応の迅速化・効率化（優先付け）	インシデント有無	公的DB1	民間DB 1	民間DB8	専用フィールド有
		Exploit有無	民間DB6	民間DB7	民間DB 1	専用フィールド有
		CVSS有無	公的DB1	公的DB 2	民間DB 1	必須上位3件
		アドバイザリ有無	公的DB1	公的DB 2	民間DB 1	専用フィールド、上位3件
コスト低減	自動化	部品ID標準	公的DB1	公的DB 2	民間DB 1	標準指定
		API・ツール提供	公的DB1	公的DB 2	民間DB2, 民間DB4	API有
		スクリプト作成容易	公的DB1	公的DB 2	—	標準ID∧API有
	情報無償提供		公的DB1	公的DB 2	その他7件	無料2件
	日本語情報提供		公的DB 2			

凡例　枠内の和集合として対象を選定

図 7-5 対象とする脆弱性 DB の選択の観点比較イメージ

(4)　マッチング手法の選択・実施

マッチング手法区分、入力 SBOM 形式、対象の脆弱性 DB の選択結果や制約条件に基づき、どの手法が利用可能か判断する。下記整理表は、実証調査時点の仕様及び事例動作確認に基づく参考判断を示す。

脆弱性DBの種類

手法区分・入力SBOMデータの種別

手法区分	SBOM形式	部品ID標準	公的DB1	公的DB2	公的DB 3	民間DB1	民間DB2	民間DB3	民間DB4	民間DB5	民間DB6	民間DB7	民間DB8
API利用	SPDX	CPE	×	○	◎	○	○	○	○	×	×	×	○
		PURL	△	△	◎	○	○	○	○	×	×	×	○
		独自ID	△	△	○	○	○	○	○	×	×	×	○
	Cyclone DX	CPE	×	○	○	○	○	○	○	×	×	×	○
		PURL	△	△	○	○	○	○	○	×	×	×	○
		独自ID	△	△	○	○	○	○	○	×	×	×	○
	SWID	SWID	×	×	×	×	×	×	×	×	×	×	×
		CPE	×	○	○	○	○	○	○	×	×	×	○
		PURL	△	○	○	○	○	○	○	×	×	×	○
		独自ID	△	○	○	○	○	○	○	×	×	×	○
Web UI利用	SPDX	CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
	Cyclone DX	CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
	SWID	SWID	×	×	×	×	×	×	×	×	×	×	×
		CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
既成ツール	SPDX (json)	CPE	×	×	×	×	×	×	×	×	×	×	×
		PURL	×	×	×	×	○ツール3	○ツール3	×	×	×	×	×
		その他	×	×	△ツール2	◎ツール2	×	×	×	×	×	×	×
	Cyclone DX (json)	CPE	×	×	×	×	×	×	×	×	×	×	×
		PURL	×	×	×	×	○ツール3	○ツール3	×	×	×	×	×
		その他	×	×	△ツール2	◎ツール2	×	×	×	×	×	×	×
	SWID	CPE	×	○ツール1	×	×	×	×	×	×	×	×	×
		PURL	×	×	×	×	×	×	×	×	×	×	×
		その他	×	×	×	×	×	×	×	×	×	×	×

Image

図 7-6 脆弱性マッチング手法の選択の参考となる一覧表（イメージ）

脆弱性マッチングにおいては、様々な脆弱性 DB が対象となるが、当面は、部品 ID 標準が複数併存することで、ID の一意性によるマッチングの課題が残ることが想定されるため、脆弱性 DB の API や WebUI を利用して、コンポーネント名、ベンダー名などの部分マッチングによる脆弱性情報の特定が現実的な方法になると考えられる。

脆弱性マッチングは、SBOM における部品情報の網羅性、部品 ID の一意性が確保されていないことなどから、脆弱性情報の検出漏れ、誤検知の可能性があるため、脆弱性マッチングの実施後に完全性を検査することは難しい場合もあるが、手動での確認などにより脆弱性マッチング結果の検証を行うことが期待される。

脆弱性特定の活動（１）～（４）は、定期的に実施し、新たな脆弱性が発見された場合に対応することが求められる。繰り返し脆弱性特定を実施する場合には、過去に対応済みの脆弱性情報やその優先付け情報と新規に発見された脆弱性情報の対応付けなどの情報管理が課題となる。今後は、VEX 情報や SBOM ツールの機能向上を通じて、そのような脆弱性情報を効率的に管理することが期待される。

7.4.2. 脆弱性対応優先付けフェーズ

脆弱性対応優先付けフェーズは以下の４ステップから構成される。

(1)脆弱性フィルタリングによる絞り込み

(2)優先付け情報の選択・取得

(3)優先付け判断ツリーに基づくカテゴリー判定

(4)優先度スコア評価

ステップごとの具体的な実施方法についてポイントを示す。

(1)　脆弱性フィルタリングによる絞り込み

外部から情報を取得し本格的に脆弱性対応優先付けを行うための工数は大きいため、脆弱性対応の要否を簡易に分かるものについては予め、仕分けを行うことが想定される。例えば、提供されるソフトウェア（部品）の脆弱性について、サプライヤーからすでに脆弱性対応済みであることが明確にされている場合は、優先付けのステップを省略し予め仕分けすることができる。今後、ベンダーから脆弱性の対応要否の情報を含む VEX 情報が提供されるようになれば、それらの情報も本ステップにおけるフィルタリングを通じて、優先付けのステップを省略することができる。

以下のステップでは、脆弱性対応が不要なものを除いた脆弱性について、外部情報を取得することで、優先付けを行う方法について示す。

(2)　優先付け情報の選択・取得

優先付けに必要となる情報の選択・取得を行う。優先付けに必要となる情報は、SBOM による脆弱性管理の費用対効果を尺度として判断することができる。費用対効果の基本構造は以下のように捉えることができる。

（脆弱性対応優先付けの尺度）∝（効果）/（コスト）=（脆弱性リスク低減効果）/（コスト）
∝（脅威発生可能性）×（脆弱性残留可能性）×（影響度）／（コスト）

SBOM を用いた効果についてはセキュリティを対象に考えた場合、脆弱性管理によるリスク低減効果と捉えることができる[31]。脆弱性リスクは、セキュリティ分野においては、事故発生可能性と事故が起きた場合の影響度（損害額の大きさ）に比例する[32、33]。事故発生可能性は（脅威発生可能性）、（脆弱性残留可能性）に比例するため、上記の比例関係で費用対効果を捉えることができる。

これらの構成要素の大きさを比較評価するための情報としては以下の表のものが挙げられる。

---

[31] SBOM の効果には、セキュリティに関わる脆弱性リスクのほか、ライセンスのコンプライアンス違反などライセンスリスクがある。

[32] サイバーセキュリティ戦略本部研究開発戦略専門調査会 講演 「社会問題から見たサイバーセキュリティ技術課題」、三菱総合研究所 石黒正揮、2019 年

[33] 情報処理学会 特集「デジタルエコノミー時代のサイバーセキュリティ」「サイバーセキュリティ経済学」、三菱総合研究所 石黒正揮、2018 年

表 7-2 脆弱性対応優先付けに必要な情報一覧

評価カテゴリー			評価項目	説明・重要性の考え方
リスク	発生可能性	脅威発生可能性(外部要因)	インシデント(有・無・不明)	実際に悪用・事件が発生しており緊急性が高い。
			Exploit コードの公開（有・無・不明）	悪用コードが公開されており、悪用される可能性が高い。
		脆弱性残留可能性(内部要因)	VEX 脆弱性ステータス（影響：有・無・不明）	脆弱性に係る部品を利用した開発者が直接評価したものであり VEX 発行時に適切なプロセス・評価基準で評価が行われる限り精度が高い。
			VEX 以外の悪用可能性独自評価（悪用：可・否・不明）	VEX が取得できない場合、独自に悪用可能性を評価する。部品開発主体の作成を前提とする VEX とは異なり、精度が低い可能性が存在する。
			アドバイザリー対処策適用可否（可・否・不明）	脆弱性に対する一般的な対処策であり、部品 ID・脆弱性 ID が完全に一致する場合以外は、悪用可能性の精度は高くない。
			脆弱性修正パッチの有無（ゼロデイ）	ベンダーにとって、脆弱性修正パッチを未提供である場合、ユーザー・調達者に対する責任が大きいため優先度が高い。
	影響度		CVSS スコア（特に影響評価）	一般的なケースにおける影響度及び深刻度の評価であり、ユーザー環境に基づく評価ではないため、精度は高くない。
			ユーザー影響度評価（情報資産の重要性 CIA）	ユーザーの情報資産(CIA)に特化した評価であり実態に基づく評価であり精度が高いと想定される。外部提供サービスは、社内システムより影響度が高い。(CIA 各要素 2,1,0 の合計値など)
			多数の製品・サービスに影響、問合せ多数	後半に影響する可能性がある。(3 段階評価 3,2,1)
コスト			サービス中断・縮退	社内外のサービス中断・縮退の影響を考慮し、タイミングを検討(3,2,1)
			ソフトウェア修正	サプライヤーの修正が遅い場合、自社で修正する場合のタイミングを検討
			修正の影響テスト・修正の適用	修正適用の影響テストが可能か検討
			悪用可能性評価コスト	悪用可能性評価をサプライヤーに代わり自社で行う場合のコストを評価し対応判断。

これらの情報を収集することにより、次のステップ以降の考え方に基づき優先付けを行うことができる。これらの情報源は主に、7.4.1(3)節に示す脆弱性 DB や SBOM ツールを候補に、各社の要求水準に関わるポリシーや投入できる予算に応じて取捨選択することができる。

(3) 優先付け判断ツリーに基づくカテゴリー判定

優先付けに必要な情報の選択・取得の結果、それらの情報を用いて脆弱性対応優先付けのカテゴリー判定（優先順序分け）を行う。そのための方法として、国際的に標準化されたフレームワークを用いることは説明責任を果たし、国際的な整合性を確保する上で重要であるため、米国 CISA により提案された脆弱性対応の優先付けを行うフレームワーク SSVC（Stakeholder-Specific Vulnerability Categorization）[34]を用いる。SSVC においては、悪用可能性、悪用効率性、技術的影響度、ユーザー影響度に関する条件分岐により判断ツリー構成し、その結果として優先付けのカテゴリー判定（４区分：即対応、通常保守より優先、通常保守、対応保留）を行う（下図）。

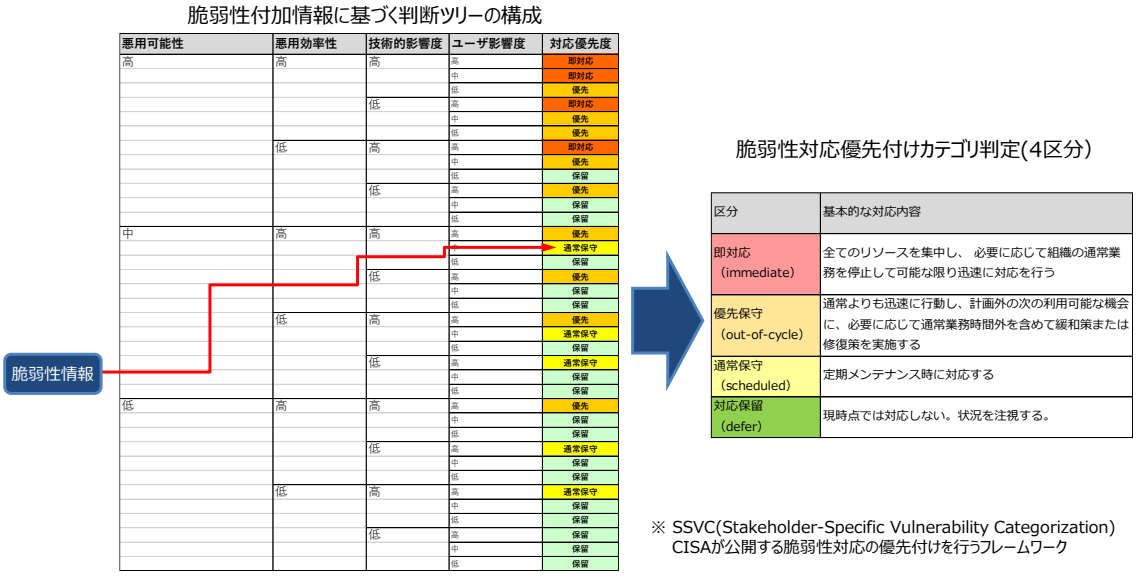

図 7-7 SSVC に基づく脆弱性対応優先付けの判断ツリーの構成と判定カテゴリー（４区分）

条件分岐の判断基準については、企業のセキュリティポリシーにより裁量の余地はあるが、経済産業省 SBOM 実証事業を通じて評価検討を行い、その考え方を整理した。各企業は自社のポリシーに応じて、本手引きに示す考え方を参考に具体的に決めることが想定される。

条件分岐の判断基準は、企業の役割や技術力によって対応が異なることが想定される。脆弱性の修正を行うのは、機器メーカーや部品サプライヤーなど実際にソフトウェア開発した組織が、自組織が開発した部分について担うことが効率的、現実的である。そのため、判断ツリー条件分岐は、開発組織、

[34] CISA, SSVC (Stakeholder-Specific Vulnerability Categorization)
https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf

ユーザー組織を区別する。また、組織における SBOM の利用や脆弱性管理に関する技術力により、現実的にできることが異なることから、技術力の高・低により区別する。以上のことから、脆弱性優先付けのための判断ツリーは、役割（開発組織、ユーザー組織）×技術力（高い、高くない）の４区分により、それぞれの考え方の参考例を示す。

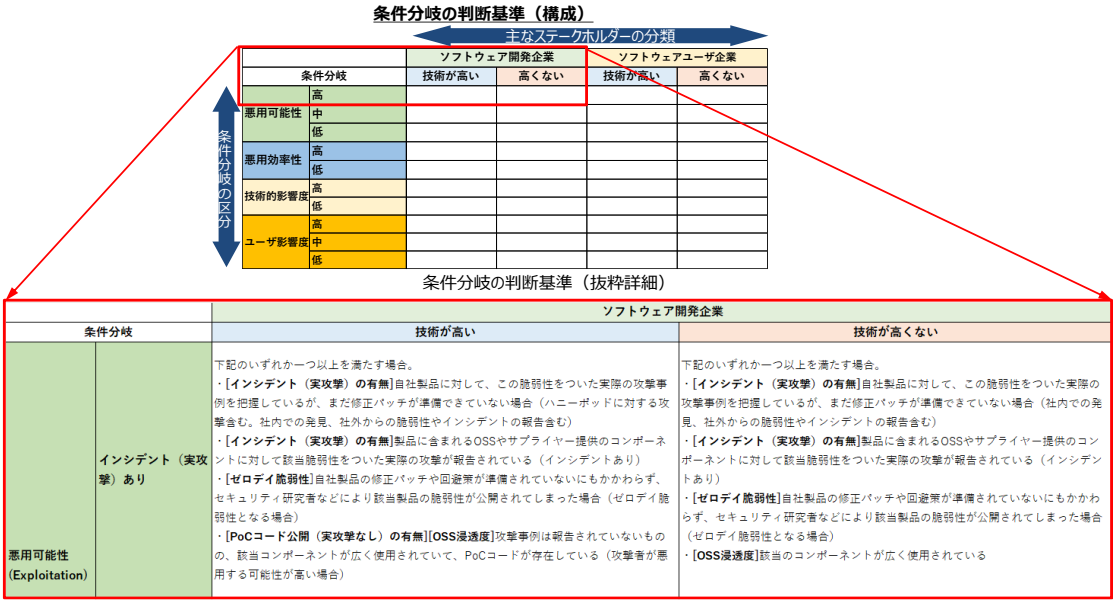

図 7-8 脆弱性対応優先付け判断ツリーの４区分ごとの判断基準の全体像

次表に、４区分ごとの各条件分岐における判断方法について示す。この表 7-3 は、表 7-2 に示す脆弱性対応優先付けに用いられる情報を基に、優先付けカテゴリーの判断を行うための具体的な方法について例示したものである。これらを参考に、企業ごとのポリシーに基づき判断基準を決定することが期待される。

表 7-3 組織カテゴリーごとの優先付け判断方法

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		**技術力が高い**	**技術力が低い**	**技術力が高い**	**技術力が低い**
悪用可能性 (Exploitation)	**高**	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無]**自社製品に対して、該当脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合（ハニーポットに対する攻撃含む。社内での発見、社外からの脆弱性やインシデントの報告含む） **・[インシデント（実攻撃）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている（インシデントあり） **・[ゼロデイ脆弱性]**自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合（ゼロデイ脆弱性となる場合）	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無]**自社製品に対して、該当脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合（社内での発見、社外からの脆弱性やインシデントの報告含む） **・[インシデント（実攻撃）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている（インシデントあり） **・[ゼロデイ脆弱性]**自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合（ゼロデイ脆弱性となる場合） **・[OSS 浸透度]**該当のコンポー	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無]**製品又は製品に含まれる OSS（SBOM から判断）に対して脆弱性をついた実際の攻撃事例が報告されている場合 **・[インシデント（実攻撃）の有無]**製品ベンダーから、悪用される可能性が高いと報告されている場合 **・[PoC コード公開（実攻撃なし）の有無][OSS 浸透度]**攻撃事例は報告されていないものの、該当製品・コンポーネントが広く使用されていて、PoC コードが存在している（攻撃者が悪用する可能性が高い場合） **・[インシデント（実攻撃）の有無]**自社の持つシステムへの攻撃の可能性について、社内外から報告されている	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無]**JPCERT/CC やニュース、ベンダーからの通知で、実際に悪用事例があることが公表されている **・[脆弱性解説]** ベンダーが修正の早期適用を推奨している **・[インシデント（実攻撃）の有無]**自社の持つシステムへの攻撃の可能性について、社内外から報告されている

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		**技術力が高い**	**技術力が低い**	**技術力が高い**	**技術力が低い**
		・[PoC コード公開（実攻撃なし）の有無][OSS 浸透度]攻撃事例は報告されていないものの、該当コンポーネントが広く使用されていて、PoC コードが存在している（攻撃者が悪用する可能性が高い場合）	ネントが広く使用されている		
	中	**・[PoC コード公開（実攻撃なし）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントの脆弱性に対して、PoC コード(Exploit コード）が存在している場合（ただし、実際の攻撃への使用は確認されていない。また PoC はあるが社内で発見された脆弱性であり、社外公開されていないことが確認されている場合は除く）	**・[PoC コード公開（実攻撃なし）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントの脆弱性に対して、PoC コード(Exploit コード）が存在している場合（ただし、実際の攻撃への使用は確認されていない。また PoC はあるが社内で発見された脆弱性であり、社外公開されていないことが確認されている場合は除く）	**・[PoC コード公開（実攻撃なし）の有無]**脆弱性をついた実際の攻撃事例は報告されていないが、PoC コードが存在している場合	上記以外

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		**技術力が高い**	**技術力が低い**	**技術力が高い**	**技術力が低い**
	低	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無][PoC コード公開（実攻撃なし）の有無]**該当脆弱性に対して、攻撃事例・PoC コードともに存在していない場合 **・[インシデント（実攻撃）の有無][PoC コード公開（実攻撃なし）の有無]**自社内で発見された脆弱性で、外部で攻撃に使用された事例が確認されていない場合	下記のいずれか一つ以上を満たす場合。 **・[インシデント（実攻撃）の有無][PoC コード公開（実攻撃なし）の有無]**該当脆弱性に対して、攻撃事例・PoC コードともに存在していない場合 **・[インシデント（実攻撃）の有無][PoC コード公開（実攻撃なし）の有無]**自社内で発見された脆弱性で、外部で攻撃に使用された事例が確認されていない場合	**・[インシデント（実攻撃）の有無][PoC コード公開（実攻撃なし）の有無]**該当脆弱性に対して、攻撃事例・PoC コードが発見されていない場合	
悪用効率性	**高**	下記のいずれか一つ以上を満たす場合。 **・[該当システムの設置場所]** 該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例：公開 WEB サーバ、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器（VPN、FW 等）	下記のいずれか一つ以上を満たす場合。 **・[該当システムの設置場所]**該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例：公開 WEB サーバ、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器（VPN、FW 等）	**・[該当システムの設置場所]**該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例：公開 WEB サーバ、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器（VPN、FW 等）	**・[該当システムの設置場所]**該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例：公開 WEB サーバ、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器（VPN、FW 等）

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		**技術力が高い**	**技術力が低い**	**技術力が高い**	**技術力が低い**
		・**[脆弱性解説]** RCE/コマンドインジェクションの脆弱性である	・**[脆弱性解説]** RCE/コマンドインジェクションの脆弱性である		
	低	上記以外	上記以外	上記以外	上記以外
技術的影響度	**高**	下記のいずれか一つ以上を満たす場合。 ・**[システムのセキュリティ機能への影響]** 該当脆弱性を用いることで、攻撃者が対象製品を備えるシステムのセキュリティ機能（ユーザー認証やロール設定によるアクセス制限、改ざん防止機能など）を無効、又は回避することが可能となる ・**[脆弱性解説]**該当脆弱性を用いることで、攻撃者が対象製品に含まれる情報を入手することが可能となる	下記以外（影響度を自社で判断することができない場合を含む）	下記のいずれか一つ以上を満たす場合。 ・**[システムのセキュリティ機能への影響]**該当脆弱性を用いることで、攻撃者が対象製品を備えるシステムのセキュリティ機能（ユーザー認証やロール設定によるアクセス制限、改ざん防止機能など）を無効、又は回避することが可能な場合 ・**[脆弱性解説]**該当脆弱性を用いることで、攻撃者が対象製品上の情報を入手することが可能な場合	（この項目は判定せず、すべて高として扱う）

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		**技術力が高い**	**技術力が低い**	**技術力が高い**	**技術力が低い**
		・**[CVSS スコア]**（上記の判定が困難な場合のみ）CVSS スコアが Critical 又は High		上記の判定が困難な場合は、以下の条件を満たす場合。 ・**[CVSS スコア]**製品開発企業（最終ベンダー）による CVSS スコアが Critical 又は High（最終ベンダーからの情報がない場合、該当脆弱性を含む OSS に関する CVSS スコアが Critical 又は High）	
	低	上記以外	・**[CVSS スコア]**影響のある OSS の CVSS スコアが Middle 又は Low	上記以外	
ユーザー影響度	**高**	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**対象製品が、社外ネットワークと社外ネットワークの接点となるシステムである（VPN 機器、FW など） ・**[対象システムの性質]**対象製品が、医療機器のクラス II/III/IV にあたる	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**対象製品が、社外ネットワークと社外ネットワークの接点となるシステムである（VPN 機器、FW など） ・**[対象システムの性質]**対象製品が、医療機器のクラス II/III/IV にあたる	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**該当脆弱性が、漏えいすることで会社や社員に致命的な影響を与える情報を扱う製品に存在する（機密度が極めて高い情報など） ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジ	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**該当脆弱性が、漏えいすることで会社や社員に致命的な影響を与える情報を扱う製品に存在する（機密度が極めて高い情報など） ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジ

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		技術力が高い	技術力が低い	技術力が高い	技術力が低い
		・**[対象システムの性質]**脆弱性の影響を受ける自社のコンポーネントは、自社内又は他社の最終製品開発チームに利用され、最終製品に組み込まれるものである（ライブラリやフレームワークなど） ・**[問合せ数]**（自社 PSIRT やサポート部門などから情報が得られる場合のみ）自社の多数の製品・サービスに影響する、又は多数の問合せをすでに受けている ・「影響度中」の条件に当てはまらない	・**[対象システムの性質]**脆弱性の影響を受ける自社のコンポーネントは、自社内又は他社の最終製品開発チームに利用され、最終製品に組み込まれるものである（ライブラリやフレームワークなど） ・**[問合せ数]**（自社 PSIRT やサポート部門などから情報が得られる場合のみ）自社の多数の製品・サービスに影響する、又は多数の問合せをすでに受けている ・「影響度中」の条件に当てはまらない	ネスに甚大な影響を及ぼす（8 割以上の社員の業務が止まるなど） ・**[対象システムの性質]**該当脆弱性が社外ネットワークと社内ネットワークの接点となるシステムに存在する（VPN 機器、FW など） ・**[対象システムの性質]**該当システムの故障や不具合が、人間の精神的・身体的健康、環境に致命的な影響を及ぼす可能性がある	ネスに甚大な影響を及ぼす（8 割以上の社員の業務が止まるなど） ・**[対象システムの性質]**該当脆弱性が社外ネットワークと社内ネットワークの接点となるシステムに存在する（VPN 機器、FW など） ・**[対象システムの性質]**該当システムの故障や不具合が、人間の精神的・身体的健康、環境に致命的な影響を及ぼす可能性がある
	中	・**[対象システムの性質]**対象製品（自社がサプライヤーとしてコンポーネントを最終製品開発ベンダーに提供している場合を除く）は、個人情報などユーザーから取得したデータや、ユーザーが入力するデータ（センサーからの情報含む）を保存・保管や、データ転送することはないと確定している	・**[対象システムの性質]**対象製品（自社がサプライヤーとしてコンポーネントを最終製品開発ベンダーに提供している場合を除く）は、個人情報などユーザーから取得したデータや、ユーザーが入力するデータ（センサーからの情報含む）を保存・保管や、データ転送することはないと確定している	下記のいずれか一つを満たす場合。 ・**[対象システムの性質]**該当脆弱性が、自社の機密情報を扱う製品に存在する ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジネスに無視できない影響を及ぼす（特定部署の業務が止まる、半数以上の社員の業務が止まるなど）	下記のいずれか一つを満たす場合。 ・**[対象システムの性質]**該当脆弱性が、自社の機密情報を扱う製品に存在する ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジネスに無視できない影響を及ぼす（特定部署の業務が止まる、半数以上の社員の業務が止まるなど） ・**[対象システムの性質]**該当システ

		ソフトウェア開発企業		ソフトウェアユーザー企業	
判断ノード		技術力が高い	技術力が低い	技術力が高い	技術力が低い
				・**[対象システムの性質]**該当システムの故障や不具合が、人間の精神的・身体的健康、環境に無視できない影響を及ぼす可能性がある(又は、その可能性を否定できない)	ムの故障や不具合が、人間の精神的・身体的健康、環境に無視できない影響を及ぼす可能性がある(又は、その可能性を否定できない)
	低	（上の二つから選ぶこと）	（上の二つから選ぶこと）	・**[対象システムの性質]**該当脆弱性を持つシステムが停止しても、自社ビジネスに軽微な影響しかない（又は影響はない）	・**[対象システムの性質]**該当脆弱性を持つシステムが停止しても、軽微な影響しかない（又は影響はない）

判断ノードの各々について、企業の既存利用のフレームワーク、業界のフレームワークを参考とすることも考えられる。

なお、優先付けは評価者により評価に違い生じる可能性があるため、個々の優先付け情報の導出プロセスや前提条件・評価基準の妥当性、評価根拠となるエビデンスの有無・内容等から、優先付け情報の検証を行うことも推奨される。

(4)　優先度スコア評価

（３）脆弱性対応優先付けのカテゴリー判定と並行して、必要に応じて定量的なスコアリングによりカテゴリー内の優先付けを行うことで詳細な優先付けを行うほか、その根拠となる付加情報をエビデンスとして整理する。スコア評価は、評価項目ごとの値（有、無、不明）などに数値を割当て、ウェイトをかけた総和（重みづけ総和）により評価する。

参考ウェイトをベースに、個社ごとの優先ポリシーに応じてウェイトを調整する。これらのウェイトを参考に、各組織の状況やポリシーに応じてウェイトをカスタマイズすることで、脆弱性ごとに重みづけ総和によりスコアを算出することが可能になる。

個社のポリシーで設定

評価カテゴリ			評価項目	値	ウェイト（重要性）	参考ウェイト
リスク	発生可能性	脅威発生可能性（外部要因）	インシデント(有・無・不明)	有		3
			Exploitコードの公開（有・無・不明）	無		2
		脆弱性残留可能性（内部要因）	VEX脆弱性ステータス（影響：有・無・不明）	無		3
			VEX以外の悪用可能性独自評価（悪用：可・否・不	可		2
			アドバイザリ対処策適用可否（可・否・不明）	可		1
			脆弱性修正パッチの有無（ゼロデイ）	有		3
	影響度		CVSSスコア（特に影響評価）	8.5		2
			ユーザ影響度評価（情報資産の重要性CIA）	3		3
			多数の製品・サービスに影響、問合せ多数	2		3
コスト			サービス中断・縮退	2		3
			ソフトウェア修正	1		1
			修正の影響テスト・修正の適用	2		2
			悪用可能性評価コスト	1		2
総合評価						

図 7-9 優先付けスコア評価の評価項目と参考ウェイト

なお、優先付けやスコアリングにおいて利用が想定される VEX 情報は、ベンダーなどから提供されることが期待されるが、現状では提供されるケースが限られていることから、VEX の取得が難しい場合には、米国 CISA が提供する悪用が確認された脆弱性情報のカタログ KEVC(Known Exploited Vulnerabilities Catalog)[35]を活用することが想定される。また、CVSS は、比較的広く利用されてい

[35] Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog

るものの、脆弱性の実際の悪用状況が考慮されていないため、CVSS を補完する脆弱性の評価指標として、FIRST（Forum of Incident Response and Security Teams）が主導して策定された EPSS（Exploit Prediction Scoring System）[36]を利用することも考えられる。

7.4.3. 情報共有フェーズ

CISA SBOM 共有ライフサイクル[37]を拡張することで、SBOM に加え脆弱性情報・付加情報を含む情報共有方法を整理する。

情報共有は以下の 2 つのステップを参考に実施内容を検討することが期待される。

(3.1)共有情報と相手の特定

(3.2)共有方法の特定と実施

以下に、これらのステップで実施する事項の参考例を示す。

[36] The EPSS Model, https://www.first.org/epss/model

[37] CISA, Software Bill of Materials (SBOM) Sharing Lifecycle Report https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report

表 7-4 情報共有フェーズのステップ

<table>
<tr><th colspan="2">プロセス・フェーズとステップ</th><th>ソフトウェア開発者</th><th>ソフトウェア利用者</th></tr>
<tr><td rowspan="4">(3.1)共有する情報と相手の特定</td><td rowspan="2">(3.1.1)共有情報の特定</td><td colspan="2">脆弱性管理のフェーズ(1)で取得した脆弱性情報、フェーズ(2)で取得した付加情報（悪用可能性、深刻度、アドバイザリー、VEX 等）、修正した SBOM 等の共有（提供又は取得）する情報を特定する。</td></tr>
<tr><td>開発者は脆弱性の再現確認、修正対応を行うため、脆弱性対応要否・優先付けの付加情報として、必要に応じてそれらの情報を提供することも想定される。</td><td>ユーザーは利用状況に応じたリスク評価を行うことで、脆弱性対応・優先付けにおける付加情報の提供を、ベンダーに対して要求することも想定される。</td></tr>
<tr><td>(3.1.2)共有相手の特定・</td><td>社内の開発部門と管理部門(PSIRT, 品質保証）及び社外（ユーザー、ベンダー）の共有相手を特定し、相手に応じた情報の整備を行う。通知は、情報提供側と取得側に応じて Push 型/Pull 型に分かれる。</td><td>ベンダー、カスタマー（サービス利用組織）の共有相手を特定し、相手に応じた情報の整備を行う。
共有相手の窓口を特定する。</td></tr>
<tr><td>(3.1.3) 共有認知・トリガー (Discovery)</td><td>開発者が先行して脆弱性特定、優先度付け、修正を行うことが期待されるため、ベンダーからプッシュ型通知することが期待される。ただし、優先度付けはユーザー利用環境に応じて判断が必要になる。共有のタイミングは、脆弱性が発見・修正された時点で行うことが期待される。</td><td>SBOM を取得済みであれば、ユーザー組織でも脆弱性特定、優先付けが可能でありユーザーからベンダーに提供要求（プル型通知）をすることも想定される。脆弱性付加情報については、開発者ではないユーザーが取得できるものが限定される場合がある。</td></tr>
<tr><td>(3.2)共有方法の特定と実施</td><td>(3.2.1)共有方法の特定 (Access)</td><td colspan="2">SBOM、脆弱性情報について、共有者間で共有方法について合意する。
SBOM については、手動、スタンドアロンツールの場合のファイル送受信と SaaS 共有に分かれる。
脆弱性情報・付加情報については CVSS 以外の標準化は進んでおらず、SaaS 対応は限定的であるため、ファイル送受信が想定される。</td></tr>
</table>

	(3.2.2) アクセス権限の特定 (Access, control)	SBOM、脆弱性情報の**機密性、権利に応じて、開示区分（非公開/一部公開/公開）、アクセス制限**について合意し、必要に応じて認証実現する。 スタンドアロン、SaaS のツール区分によって開示区分、アクセス制限などの管理について合意・実装する。 サプライチェーンを通じた SBOM の共有については、SaaS による共有がアクセス範囲を限定して、リアルタイムで効率的に共有することが可能なSaaSによる方法が効果的であるが、SaaSコストとの費用対効果の評価が必要である。
	(3.2.3)共有実施 (Transport)	共有方法、アクセス権限等の合意に基づき、SBOM、脆弱性情報・付加情報の共有を実施する。 SBOM については、CISA 文書[1]に示されるように、**手動転送（メール等）、一部自動化、標準ルールに基づく自動化のレベル分け**がされているが、自動化については、SaaS 型ツールが該当する。 SW サプライチェーンの中で過去に SBOM を共有している場合、脆弱性マッチングの検証の結果、対応が不要と判明した脆弱性についても通知し、サプライチェーン全体で対応を停止する。

7.4.4. 脆弱性対応フェーズ（暫定対応・根本対応）

脆弱性対応は、脆弱性の修正を伴う根本対応と、回避策による即時性が求められる暫定対応に分けられる。脆弱性の修正は、一般的には、ソフトウェアの開発者が実施することが想定される。SBOM/VEX 修正は根本対応時に必要になる。様々な事業者は、ソフトウェアの開発と利用の両方を担うことが多く[38]、立場に応じてそのバランスは異なる。開発と利用の立場に応じて、下記のプロセスの組合せの対応が求められる[39]。

(4.1)脆弱性暫定対応

(4.2)脆弱性根本対応

以下に脆弱性対応フェーズで実施する事項の参考例を示す。

[38] サービス事業者であっても、システム部門が開発を行うケースがある。部品サプライヤーでも、さらに部品を利用するケースがある。

[39] 調達先の開発者が、OSS ソフトの修正や SBOM 修正を行わない場合、調達元が開発者と同等の対応が求められることを事前に認識する必要がある。

サービス事業者
SI事業者
機器製販者
部品サプライヤ

プロセス・フェーズとステップ		ソフトウェア開発	ソフトウェア利用
(4.1)脆弱性暫定対応	**(4.1.1)暫定策の検討**	• 脆弱性修正前の暫定対応策の検討（利用中断、縮退動作、回避策等）。 回避策としては、防御機構の追加変更、設定変更、利用者制限など多様である。	• ユーザ組織内での暫定対応策の検討（利用中断、縮退動作、回避策等）。 • ベンダーへの暫定対応策の確認
	(4.1.2) 暫定策の適用	• 供給先（ユーザ組織を含む）への暫定対応策の周知 （SBOMの修正はなし）	• ユーザ組織内の暫定対応策とベンダーが提示する暫定対応策を比較し、意思決定を行う。 • 社内サービスと社外サービスにより影響度の大きさを考慮して暫定策を判定する。 （SBOMの修正はなし）
(4.2)脆弱性根本対応	**(4.2.1) 根本対応の実施**	• 脆弱性が自社開発部分の場合、脆弱性の修正 • 脆弱性がサプライヤー開発部分の場合、サプライヤーに修正を依頼し、自社の開発部分に、脆弱性修正を適用する。	• ベンダーへの修正を要求する。 • ベンダーからの修正パッチを適用する。 • 重要インフラ・サービスの場合、修正適用の期限などの目標値を設定している。
	(4.2.2) SBOM・VEX更新	• 脆弱性の修正に伴い、SBOMを更新する • 脆弱性の修正に伴い、VEXの作成・更新を行う。	• 最終ベンダーから提供された脆弱性修正に対応してVEXの修正を行い、以降の脆弱性管理において誤検知を回避する。 （通常はユーザ組織は、ソフトウェアの脆弱性修正を行わないためSBOMの修正は行わない）
	(4.2.3) SBOM・VEXの共有	• 供給先にSBOM/VEXを共有する。 • 必要に応じてSBOMの履歴管理を行う。	• ベンダーから脆弱性修正に伴い更新されたSBOM/VEXを取得する。 • 必要に応じてSBOMの履歴管理を行う。

図 7-10 脆弱性対応のステップとステークホルダーごとの実施内容例

以上のフェーズから構成されるステップを通じて SBOM を活用した脆弱性管理を行うことができる。

8. 付録：SBOM 対応モデル

8.1. 目的と背景

8.1.1. 目的

本章では、SBOM の生成・活用に関する対応範囲の違いを可視化する方法について示し、それを用いることで、ソフトウェア取引において、脆弱性管理などのソフトウェア管理レベルの高い製品が評価され、選別されることにより、SBOM に対応する供給者のインセンティブを向上させ、SBOM の普及促進や、SBOM 対応レベルの適正化を進める仕組みとその活用方法について示す。

SBOM をどのように導入するか（How-To）については手引書(1～6 章)で示しているが、本章では、SBOM 対応レベルの可視化を通じて、SBOM について、何をすべきか（What）、なぜすべきか(Why)のインセンティブを確保する仕組みを提供することを目的としている。

8.1.2. 問題認識

SBOM の活用は、実施するかしないかの 2 択ではなく、ソフトウェアの構成部品の特定範囲やその部品情報に基づく脆弱性管理の範囲に応じて多様な選択肢により決まるもので、多数の対応レベルが存在する。再利用部品の特定は技術的にもコスト的にも課題が大きく、どの程度構成部品を特定できているかによって、脆弱性管理のレベルに大きな影響を与える。また、SBOM 対応レベルに応じてコスト・効果が大きく異なるため、分野のリスクに応じてどこまで対応すればよいか適正レベルを判断することが重要になる。

このような SBOM 対応レベルの違いについて製品間で比較可能な可視化の仕組みがなければ、適正なレベルの SBOM 対応を行うインセンティブが働かない。例えば、高いコストをかけて高いレベルの SBOM 対応レベルを実現しても、ソフトウェアの調達者から SBOM 対応レベルの高さと価値が認識され、比較可能でなければ、SBOM 対応レベルの評価に基づく製品選択にはつながらないため、高いコストをかけて SBOM に対応するインセンティブは働かない。SBOM 対応レベルの違いが比較可能な共通フレームワークで可視化されれば、高いレベルの脆弱性管理が求められる分野においては、それに対応した SBOM 対応レベルの高い製品の選別が可能となり、分野のリスクや要求レベルに応じて SBOM 対応レベルの適正化が促進する。

これまでは、SBOM 対応レベルについて比較可能な共通的に利用できる枠組みが存在しなかったため、適切なレベルの SBOM に対応するインセンティブが働かなかった。このようなことから、SBOM の生成・活用に関する対応範囲と対応レベルについて、SBOM 対応のインセンティブを高める仕組みとして、比較可能で共通的に利用できる可視化のフレームワークの提供が求められる。

8.1.3. 想定読者

本章の SBOM 対応モデルは、サプライチェーンを通じてソフトウェアと SBOM の供給者と調達者の双方が、想定読者となる。双方の取引において、ソフトウェアのセキュリティ品質（構成管理・脆弱性管理レベル等）を可視化し、合意するためのコミュニケーション手段として用いられる。ソフトウェアや SBOM の供給者としては、開発・運用部門やセキュリティ担当部門(PSIRT)を対象とし、ソフトウェアの調達者としては、ユーザー企業、開発企業の調達部門、開発部門、品質保証部門、セキュリティ担当部門の担当者を対象とする。また、SBOM 対応モデルの活用を通じ社会全般や取引相手に対して説明責任が求められる経営者・CISO にとっても重要である。本章は、第 1 章から第 6 章までの SBOM に関する基礎を理解した人が、次のステップとしてソフトウェアの取引などにおいて活用するものであり、 第 6 章までの知識を前提とする。

8.1.4. 本章の構成

本章の構成は以下のとおりである。8.1 では、目的と問題認識について述べ、全体の要点を簡潔に示す。8.2 では、SBOM 対応モデルとその基盤となる SBOM 可視化フレームワークについてまとめる。8.3 では SBOM 対応モデルの位置づけと活用方法についてまとめる。8.4～8.6 では、分野ごとの法制度や前提条件をまとめ、SBOM 実証の結果に基づき整理した分野ごとの SBOM 対応モデルを示し、分野ごとの活用方法や留意点についてまとめる。

8.2. SBOM 可視化フレームワークと対応モデル

8.2.1. SBOM 対応モデルとは？

「SBOM 対応モデル」とは、SBOM を用いた部品の特定、脆弱性管理において期待される実施項目のうち、どの範囲まで対応すると良いのか対応範囲を可視化し、推奨項目や要求項目の範囲を示すものである。SBOM の項目は多様であり、SBOM 対応範囲に応じてコストと効果が大きく異なるため、産業分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。その妥当な対応範囲の案を示すものが SBOM 対応モデルである。

例えば、SBOM によるソフトウェア部品の特定範囲は、委託開発先やサードパーティ部品ベンダーの範囲までソフトウェア部品を特定するかどうか、また、それらの主体が直接利用する部品のみを対象とするか、再利用する部品も対象とするかなどによって管理できる部品の範囲は大きく異なる。部品の特定範囲が異なれば、脆弱性の検出範囲もそれに応じて異なるため影響が大きい。

8.2.2. 基本的な考え方と期待される効果

サプライチェーンを通じて開発されるソフトウェアの管理を効率化するための基盤として、SBOM は有効である。SBOM を用いることで、部品構成に基づくソフトウェアの管理や脆弱性管理を効率化するとともに、脆弱性等のリスクを低減することが可能になる。SBOM の活用においては、SBOM を導入するか

しないかの二択では無く、SBOM により特定される部品の範囲や脆弱性管理の範囲などどこまで対応できているか違いを可視化することが重要である。分野や用途に応じて脆弱性の影響を受けるリスクは大きく異なり、SBOM の対応範囲に応じて、脆弱性が残留するリスクが異なるためである。

SBOM 対応範囲について、比較可能な共通的なフレームワークによって可視化し、取引においてそれを活用することで、以下のような効果が得られる。まず、ソフトウェアの供給者と調達者の間では、ソフトウェアに加えて、それに対する SBOM 及び SBOM 対応範囲とその対応レベルをセットでやり取りする。

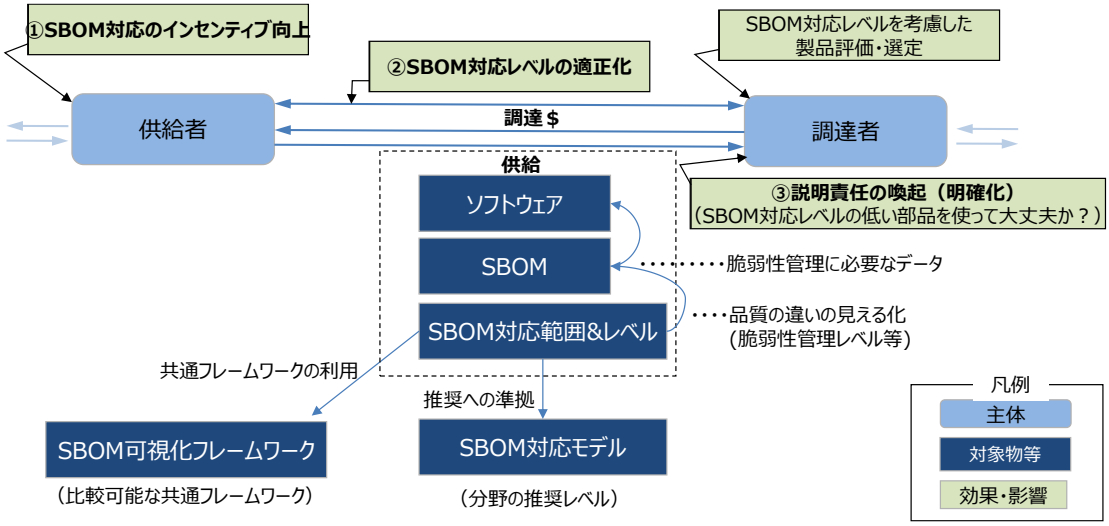

図 8-1 SBOM 対応モデルの利用者の関係と効果

SBOM 対応範囲を可視化することの効果：

① **<u>調達者・供給者の双方にとってリスクに応じた SBOM 対応レベルへ適正化</u>**

分野・用途によって異なるリスクに応じて、製品価格に反映されるコストと SBOM 対応範囲（脆弱性管理のレベル）のバランスから、適正な SBOM 対応レベルへと調整が進む。例えば利用時のリスクが低い製品については、最小限の SBOM 対応範囲に留めるなど、コストを抑えることができる。

② **<u>供給者にとっての SBOM 対応のインセンティブ向上</u>**

SBOM 対応範囲を可視化することで脆弱性管理レベルの高さを示すことが可能になる。これにより調達者の評価が高まり、製品の価値が高まる。SBOM 対応は、製品の価値を高める手段となり、供給者にとってのインセンティブを向上につながる。ただし、調達者による SBOM 対応範囲の要求は、調達者が一定の負担をするなど供給者に過剰な負担とならない仕組みが期待される。

③ **<u>調達者の意識の向上・説明責任の喚起</u>**

調達時に SBOM 対応範囲を確認して取引を行うことが一般化すれば、調達者の SBOM 対応に関する意識の向上につながる。SBOM 対応範囲を可視化し、脆弱性管理レベルが分かれば、一般社会や取引先への説明責任を果たす機会につながる。

サプライチェーンを通じて SBOM 作成のコストを負担する者と、SBOM を用いた脆弱性管理の便益

を受ける者が異なるため、それらの間で適正な対価が支払われなければ SBOM の普及の障害となる。分野に応じて SBOM の要求レベルは異なり、重要インフラ分野など、調達者が高いレベルの SBOM を要求する場合、供給者は、高いレベルの SBOM を作成するために負担しなければならないコストに対して、調達者から支払いを受けなければ、継続的な事業は成り立たなくなる。このように、SBOM の普及促進のためには、技術やツールの進歩だけでは解決できない課題がある。

SBOM 対応範囲の可視化は、サプライチェーンを通じた取引における供給者、調達者のそれぞれにとってインセンティブを高める効果がある。SBOM 対応範囲が比較可能な共通のフレームワークで可視化されなければ、調達時の比較情報として利用されないため、コスト高となる SBOM 対応レベルへのインセンティブが十分に働かないことになる。

8.2.3. SBOM 可視化フレームワーク

(1) 可視化フレームワークの構成

SBOM 可視化フレームワークは、SBOM の生成・活用に関する対応項目の選択肢について、どこまで対応しているかそのレベルを可視化するための枠組みである。SBOM による脆弱性等のリスク管理の効果とコストは、ソフトウェアにおいて利用される部品の範囲と部品情報に基づく脆弱性管理等の範囲によって決まるため、SBOM の対応範囲を可視化することが重要になる。これによりソフトウェアの脆弱性リスクにどの程度対応できているかについて判断するための参考指標として用いることを目的としたものである。

SBOM 対応範囲の可視化フレームワークは、SBOM 生成・活用に関する各種適用区分に関する対応項目選択肢とそれらの対応項目選択肢の対応状況の組合せとして可視化する SBOM 対応範囲の 2 つから構成される。その関係を示したものが下図である。

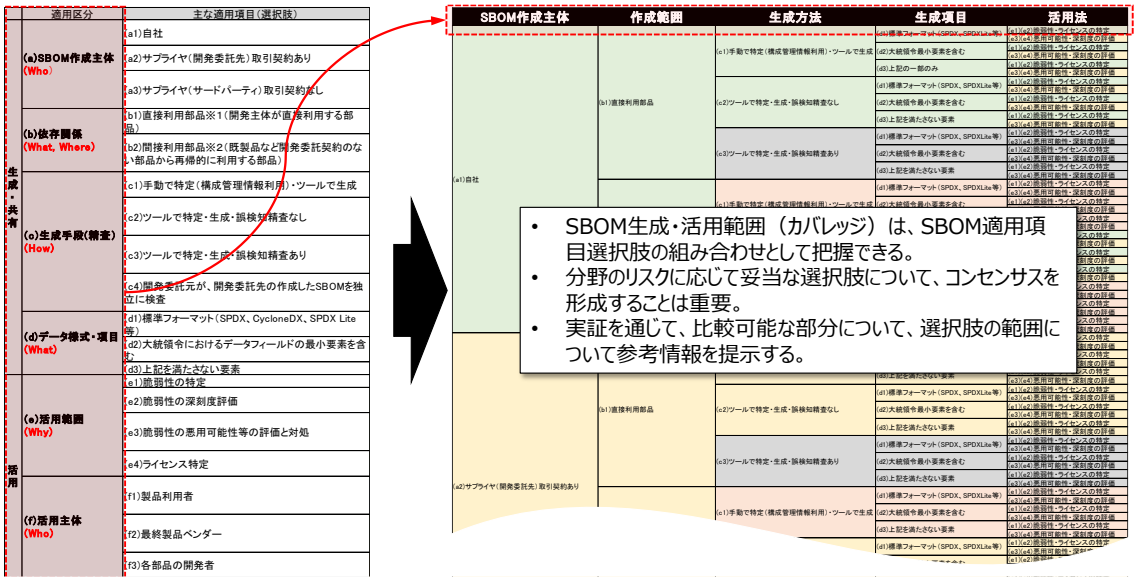

図 8-2 SBOM 対応範囲の可視化フレームワーク（イメージ）

以下では、これらの要素となる SBOM 対応項目選択肢と SBOM 対応範囲について具体的に示す。

(2)　SBOM 対応項目の選択肢

SBOM 対応項目の選択肢は、SBOM の生成・活用などの個々のフェーズで、コスト・効果に影響を与える主要な選択肢を整理したものである。SBOM を活用した構成管理・脆弱性管理の全体の対応範囲と達成度は、これらの選択肢の組合せとして特定することができる。SBOM 対応項目の選択肢については、以下のような手順で抽出・整理した。

1) SBOM に関する主要な文献からの抽出

- NTIA: SBOM at a Glance[40]
- NTIA: SBOM Options and Decision Points[41]
- NTIA: SOFTWARE BILL OF MATERIALS[42]
- CISA: Types of Software Bill of Material (SBOM) Documents[43]
- CISA: Software Bill of Materials Site (SBOM) [44]
- NIST: Software Security in Supply Chains: Software Bill of Materials (SBOM)[45]
- SPDX: SPDX® Specification Version 2.3[46]

2) SBOM に関する国内外の実証成果からの情報抽出

- NTIA: How-To Guide for SBOM Generation in Healthcare [47]
- 経済産業省: 2021 年度実証結果

3) SBOM 対応項目の選択肢（案）の整理

(1)、(2)の情報に基づき、SBOM の作成・活用に係る主な対応項目について抽出し、SBOM 対応項目選択肢（案）を整理。

---

[40] https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf

[41] https://ntia.gov/sites/default/files/publications/sbom_options_and_decision_points_20210427-1_0.pdf

[42] https://ntia.gov/page/software-bill-materials

[43] https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

[44] https://www.cisa.gov/sbom

[45] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

[46] https://spdx.github.io/spdx-spec/v2.3/

[47] https://ntia.gov/sites/default/files/publications/howto_guide_for_sbom_generation_v1_0.pdf

4) SBOM の分野ごとの実証

経済産業省: 2022 年度 SBOM 実証において、医療機器分野、自動車分野、ソフトウェア製品分野の実証企業、参加業界団体からのSBOM 対応項目選択肢（案）に対する意見を基にSBOM 対応項目選択肢（案）を改訂。

5) 経済産業省ソフトウェアタスクフォースの意見（2022 年度第 7～9 回）

ソフトウェアタスクフォースにおける SBOM に関する意見、SBOM 対応項目選択肢（案）に対する過不足に関する意見確認。

6) SBOM 対応項目選択肢（整理案）の策定

(1)～(5)の結果を基に、2022 年度までの調査・検討結果に基づき最終的な SBOM 対応項目選択肢（最終案）を整理。

以上の検討の結果整理した SBOM 対応項目選択肢（整理案）を以下に示す。SBOM 生成・活用における対応項目の選択肢は、5W1H の形式で、網羅性を確保するように整理している。以下の整理案では、SBOM 適用区分について、主要な適用項目（選択肢）を整理し、それぞれの項目に関するコストについて大中小の 3 段階に分類しその理由を示している。

表 8-1 SBOM 対応項目選択肢（整理案）

	適用区分	主な適用項目（選択肢）	コスト	主な実施内容とコスト要素
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社	小	自社開発で直接利用する部品を構成ファイルなどから特定し、SBOMを生成する。コード改変部品を含む。
		(a2)サプライヤ（開発委託先）取引契約あり	中	取引契約のある開発委託先のソフトウェアで利用する部品のSBOMを生成する。
		(a3)サプライヤ（サードパーティ）取引契約なし	大	取引契約によるSBOMの要件化できないOSSや既成部品ベンダーがSBOMを作成する。(b2)(c2)
	(b)部品範囲 (What, Where)	(b1)直接利用部品※1	小	開発者が直接利用する部品を構成ファイルなどから特定し、ツールなどでSBOMを生成する。
		(b2)間接利用部品※2	大	サードパーティ部品について、再帰的に利用される部品に対してSBOMを生成する。
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成	小	直接利用する部品情報を構成ファイルなどを用いて作成する。
		(c2)ツールで特定・生成・誤検知精査なし	中	ツールを用いてSBOMを生成し、精査は省略する。ツールの利用は再帰部品のSBOM生成を主に想定するため商用ツールの利用を想定する。
		(c3)ツールで特定・生成・誤検知精査あり	大	商用ツールを用いてSBOMを生成し、ソースコードレビューを行い、誤検知、検出漏れの精査を行う。（再帰利用部品を含む）
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査	大	開発委託元が、開発委託先の作成したSBOMを受け入れる際に、ツールなどで独立してSBOMを作成するなどして信頼性を検査する。
	(c')生成手段（部品検出手法）	依存関係解析	中	パッケージマネージャ等の構成情報を静的に解析する。
		ファイル照合	中	ハッシュ値当を用いてソースコードのファイル単位の一致を検出する。OSSのライブラリの検出なども含む。
		スニペット解析	大	ソースコードの部分的な文字列一致や類似性により検出する。
		バイナリ解析	大	バイナリファイルのビットパターンなどをもと類似性を検出する。
		実行形式内部の再帰的な依存解析	大	実行形式内にリンク済みのライブラリについて、そのライブラリをビルドする際の依存解析を再帰的に行う。
		上記に対応しない。	小	予め認識している部品をSBOMに変換する。
	(c'')生成手段（対象ソフト種別）	開発時に確定する部品	小	スタティックライブラリ、アプリケーション
		実行時に確定する部品	中	ランタイムライブラリ、サービス（ローカル、外部クラウド）、OS、ミドルウェア、実行環境（コンテナ、VM、APサーバ）
		周辺ツール環境	大	開発運用で使用するツール（インストーラ、アップデータ、配布パッケージ、開発環境、ツールチェーン、SBOMツール）
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）	中	SPDXなどの標準フォーマットで作成する。
		(d2)大統領令におけるデータフィールドの最小要素を含む	中	大統領令におけるデータフィールドの最小要素を含むSBOMを作成する。
		(d3)上記を満たさない要素	小	独自の最小限の要素を作成する。
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定	小	NVD, JVN等のDBを対象として脆弱性の検索・特定を行う。
		(e2)脆弱性の深刻度評価	中	CVSS値をベースとした深刻度を評価し、脆弱性対応の優先度を設定する。
		(e3)脆弱性の悪用可能性等の評価と対処	中	VEX情報等を用いて悪用可能性、脆弱性対処の必要性を評価する。必要に応じて対処策等のアドバイザリを発行する。
		(e4)ライセンス特定	中	ライセンスの特定と規約の取得を行う。
	(f)活用主体 (Who)	(f1)製品利用者	小	脆弱性が特定された場合、利用を中断し、ベンダーによる修正を待つ。業務中断コストも考慮すれば損害は大きい。
		(f2)最終製品ベンダー	中	利用者に脆弱性を通知するとともに、開発者への修正依頼、修正後のビルド・利用者への提供を行う。必要に応じて当局、ISAC等に報告する。
		(f3)各部品の開発者	大	開発者は、脆弱性の監視と修正を行い、調達者に修正版を提供する。必要に応じて当局、ISAC等に報告する。

※1：直接利用部品（直接部品）：サプライチェーンにおいて契約関係のある開発者が直接利用する部品

※2：間接利用部品（間接部品）：サプライチェーンにおいて契約関係のないサプライヤー（サードパーティ）が提供する部品から再利用される部品

※3：コストは「主な実施内容とコスト要素」に基づき３段階に分類。「主な実施内容とコスト要素」列の赤文字は、実証において改訂した箇所

(3)　SBOM 対応範囲の可視化

SBOM を生成・活用の対応範囲に応じて、脆弱性管理等の全体的な達成度を示す。SBOM 対応範囲は、SBOM 対応項目の選択肢の組合せとして可視化できる。それらすべての組合せの数は大きくなるが、主要な選択肢を抽出しそれらの組合せとして可視化することができる。その例を下表に示す。可視化の色分けに関する凡例は、表 8-3 に示す。SBOM 適用区分ごとの選択肢は、択一ではなく、対応する範囲について複数選択可能であり、SBOM 対応範囲は、これらの表全体により可視化・定義する。SBOM 対応範囲の達成度を指標化するものが「SBOM 対応レベル」である。SBOM 対応レベルを定義する方法としては、適用区分ごとにウェイトを設定し、対応可能な項目（緑）の重み付総和によりスコアリングすることが想定されるが、簡易的に評価する場合、表全体の項目数に対して対応する項目（緑）の割合で定義することなどが考えられる。

表 8-2 SBOM 対応範囲の可視化･定義（例）

(a)作成主体	(b)部品範囲	(c)生成手段	(d)生成項目	(e)活用範囲
(a1)最終ベンダー	(b1)直接利用部品	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
	(b2)間接利用部品	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
(a2)サプライヤ(開発委託先)取引契約あり	(b1)直接利用部品	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
	(b2)間接利用部品	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
(a3)サプライヤ(サードパーティ)取引契約なし	(b1)開発者自身	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
	(b2)開発者以外(調達者、利用者)	(c1)手動で特定(構成管理情報利用)･ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c2)ツールで特定･生成･誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
		(c3)ツールで特定･生成･誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性･ライセンスの特定 (e3)(e4)悪用可能性･深刻度の評価

SBOM 対応項目選択肢の各適用区分について対応の状況に応じて以下の４区分に色分けして可視化している。

表 8-3 SBOM 対応範囲における対応項目選択肢の対応区分

対応区分	色	対応状況説明
対応	緑	選択肢を実施する又は実施可能
部分対応	黄色	選択肢を一部実施する又は一部のみ実施可能
対応困難	オレンジ	選択肢を実施しない又は実施が困難
不要又は対象外	グレー	他の項目の実施により対応されるため実施不要

8.3. SBOM 対応モデルと活用方法

8.3.1. SBOM 対応モデルの位置づけ

SBOM 対応モデルは、SBOM 可視化フレームワークを用いて、産業分野や用途ごとのリスクに応じて、SBOM 対応範囲についてどこまで実施すべきかその推奨範囲又は要求範囲としてモデル（参考例）を示すものである。分野によりリスクや前提となる法制度等は異なり、また、SBOM 対応範囲によって脆弱性管理等の効果とコストは大きく異なるため、SBOM 対応モデルは分野ごとに異なることが想定される。

SBOM 可視化フレームワークと SBOM 対応モデルの関係を示したものが下図である。

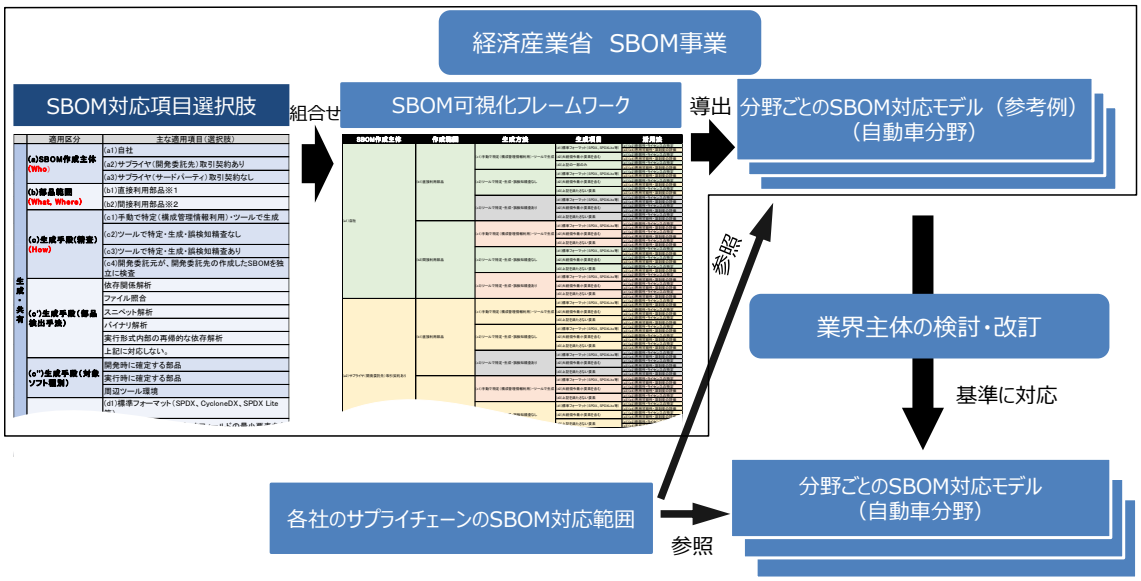

図 8-3 SBOM 対応モデルと関連する要素の関係

SBOM 可視化フレームワークは、SBOM の作成範囲・活用範囲などの対応範囲について可視化す

る汎用的な枠組みである。分野ごとの SBOM 対応モデルは、経済産業省 SBOM 事業における実証を通じて、産業分野ごとの法制度などの前提条件や、SBOM 対応のコスト・効果に基づくフィージビリティを考慮し、期待される SBOM 対応範囲の参考例を提示するものである。本章で示す SBOM 対応モデルは、規制分野の要求事項を満たすことを保証するものではなく、実証の結果、参考例を示すことを目的としたものである。規制分野については、規制当局の審査機関や業界のステークホルダーにより検討・精査を通じて分野ごとの SBOM 対応モデルの改訂を行うことが想定される。

本枠組みを用いて、SBOM 実証において、分野ごとの法制度、取引形態、開発形態などの前提条件を基に、コストと効果の計測評価を行い、分野ごとに妥当と考えられる SBOM の適用範囲（案）を示したものが「分野ごとの SBOM 対応モデル（参考例）」である。規制分野以外については、各社はサプライチェーンを通じてこのような SBOM 対応モデル（参考例）を参考に、自社の SBOM 対応範囲を決定することができる。いずれの SBOM 対応モデルも、関連分野の法制度・規制に準拠していることが求められる。このような業界確定版が策定された場合には、各社はそうした SBOM 対応モデルを参照し、必要に応じて、SBOM 対応項目を追加し、ソフトウェアや SBOM の付加価値を高めることができる。

SBOM 可視化フレームワークは、あくまでも、SBOM 対応範囲を可視化する手段を提供するものであり、最終的な SBOM 対応範囲は、業界ごとの検討を通じ精査を行うことが期待される。

8.3.2. 活用方法

8.2.1 に基づき、SBOM 可視化フレームワークと SBOM 対応モデルの活用方法について示す。サプライチェーンを通じたソフトウェアの調達における活用方法と可視化の影響を図示したものが下図である。

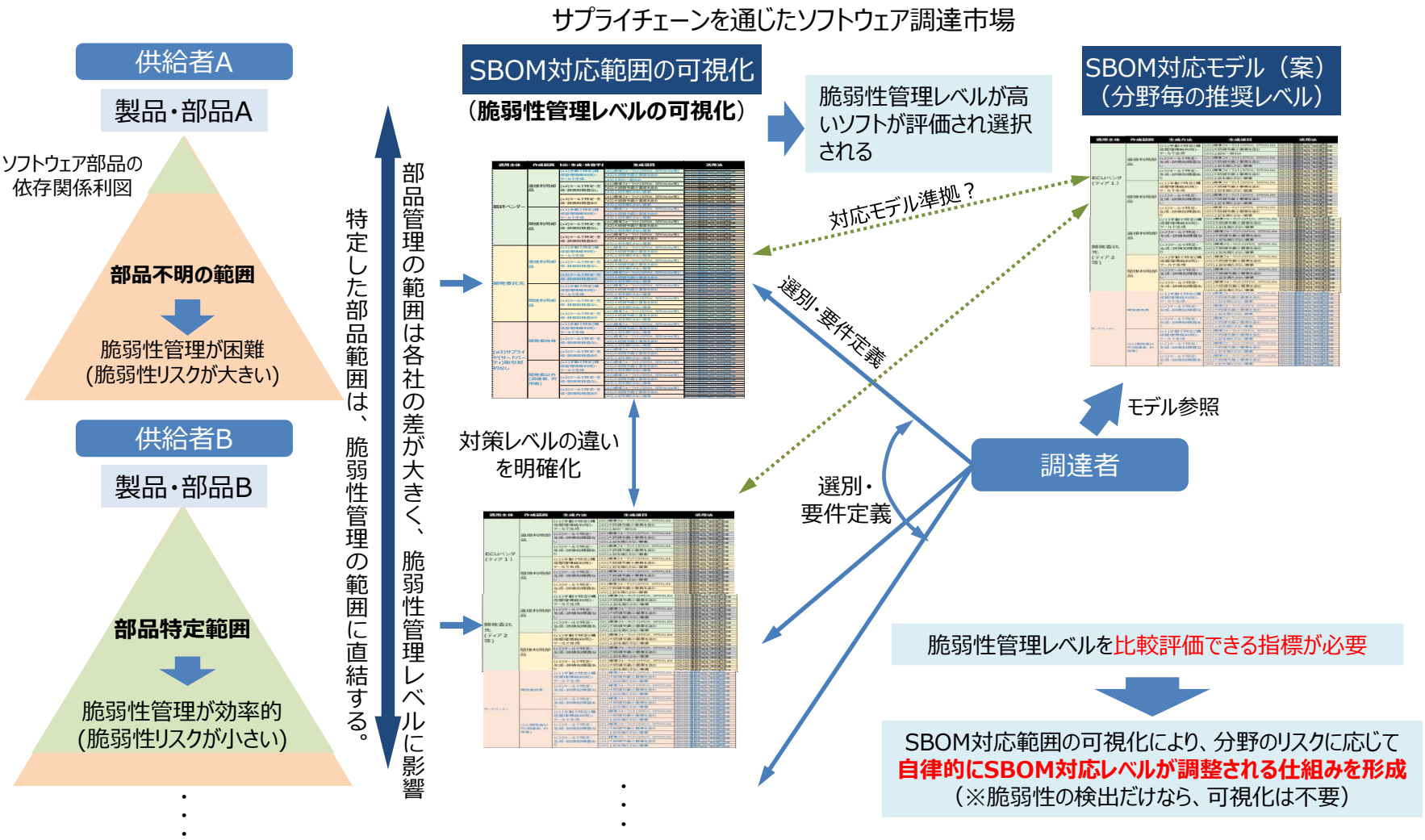

図 8-4 SBOM 対応範囲の可視化を通じた SBOM 対応のインセンティブの向上（イメージ）

図においては、ソフトウェア調達における製品・部品の供給者と調達者の関係から、SBOM のインセンティブ向上を通じて SBOM を普及させる仕組みの全体像（イメージ）を示している。

供給者により提供されるソフトウェアの脆弱性管理（脆弱性リスク）レベルは、ソフトウェアの構成部品の特定範囲や部品情報に基づく脆弱性管理の範囲などにより決まるものである。ここでは、図左側の供給者側に示した三角は、そのイメージを示すための一例として、構成部品の特定範囲の大小の違いを示している。このようなソフトウェアの脆弱性管理レベルの違いを可視化するものが、図中央の、SBOM 可視化フレームワークにより SBOM 対応範囲を可視化したものである。SBOM 対応範囲を可視化した表の緑色のカバー率が、脆弱性リスクを比較評価するための参考指標することができる。

SBOM 可視化フレームワークの使い方は、ソフトウェアの受発注が、既製品販売か、委託開発かによって異なる。既製品売買の場合、ソフトウェアに SBOM と SBOM 対応範囲及び SBOM 対応レベル（SBOM 対応項目選択肢全体のうち対応できる割合）を付随して提供することにより、調達者による選別を受けることとなる。調達者は、複数の供給者による類似ソフトウェアの価格、機能、SBOM 対応レベルを比較して製品選定を行うことになる。これにより、調達者のニーズに応じて、SBOM 対応レベルの高いものが評価されることになり、ソフトウェア提供者の SBOM 対応のインセンティブを向上させることにつながる。一方で、委託開発の場合、調達者は、SBOM 対応範囲のカバー率が、委託開発先と SBOM 対応範囲カバー率を協議し要求事項として合意することが考えられる。

当該分野において SBOM 対応モデルとして推奨範囲、要求範囲が決められている場合には、SBOM 対応範囲を SBOM 対応モデルに準拠させることが求められることになる。また、SBOM 対応モデルが決められた分野においても、プラスアルファの追加的な SBOM 対応により付加価値を高めてソフトウェアを提供するなどのインセンティブの向上にもつながる効果がある。

8.4. SBOM 対応モデルの参考例（自動車分野）

分野ごとの SBOM 対応モデルの章では、SBOM に係る法制度・基準の概要、実証に基づき整理した SBOM 対応モデル（案）、活用における留意点についてまとめる。

8.4.1. 法制度・基準の概要

自動車分野では、国連欧州経済委員会の「自動車基準調和世界フォーラム（WP29）」における分科会「自動運転（GRVA）」で取りまとめられた規則（UN-R155、UN-R156）を踏まえ、国内では、2022 年 7 月より当該規則の適用が求められている。当該規則において SBOM に係る要件は規定されていない。日欧など型式認証で要求される国連協定規則 UN-R155 から参照される ISO/SAE21434 では、要求事項の例示としてソフトウェアの構成管理が挙げられる。

米国では、 NHTSA が 2021 年初にガイダンスのドラフトが公開し、パブコメを実施。OEM に対し、ECU や各車両に使用されるソフトウェアコンポーネントに関する SBOM の作成・維持を求める要件が含まれており、今後 SBOM が推奨化される見通しである。

SBOM に係る法制度を含む自動車サイバーセキュリティの法制度の関係を整理すると以下のようになる。

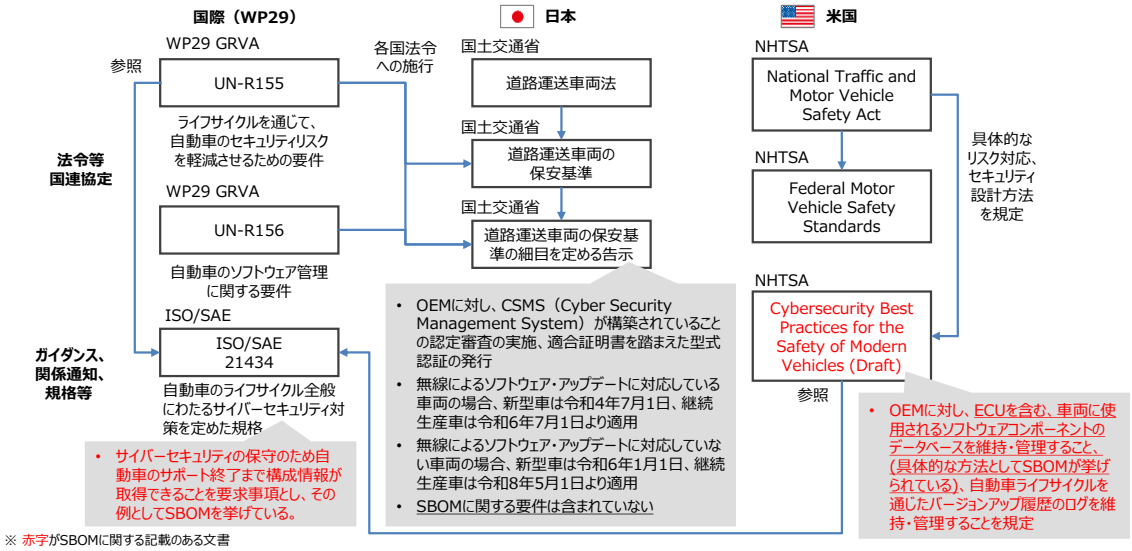

図 8-5 自動車分野の SBOM に係る法制度の関係整理

8.4.2. 実証に基づき整理した対応モデル（案）

自動車分野では、国連協定規則 UNR-155 で参照される ISO/SAE21434 において要求事項

の例示としてサイバーセキュリティの保守のためソフトウェアの構成情報が挙げられており、NHTSA が 2021 年初にガイダンスのドラフトでは、SBOM の作成・維持を求める要件が含まれているため、今後は、SBOM による構成管理が求められていくものと考えられる。

経済産業省 2022 年度 SBOM 実証においては、以下のような点に基づき SBOM 対応モデル（参考例）について整理した。ここでは実証の対象となった ECU ベンダーであるティア 1 サプライヤー及び ECU ソフトウェアサプライヤー（受託開発）を対象として、自動車分野で求められる構成管理や技術的なフィージビリティを考慮して SBOM 対応モデル（案）を整理した。

SBOM 対応モデル（案）の整理における考え方の要点は以下のとおりである。

- 自動車サイバーセキュリティ標準 ISO/SAE21434 におけるソフトウェアの構成管理の要求に基づき、開発委託先サプライヤーも含めて SBOM 生成を実施するものとする。
- サードパーティサプライヤーについては、取引契約の関係から SBOM を要求することは困難であるため必須とはしない。
- ツール生成の SBOM には誤検知が含まれる可能性があるので、十分に SBOM の効果を得るためにはツールで特定した部品の誤検知精査は必要と判断したため、SBOM 生成方法は、手動による特定に加え、「ツールで特定・生成・誤検知精査あり」の項目を対象とする。
- 間接利用部品に対しても、パッケージマネージャーを利用するなどして手動による特定も一部実施可能であると判断したため、間接利用部品について部分適用とした。
- ティア 2（ECU ソフトウェアサプライヤー）においても、対象ソースコードを所持しておりティア 1 と同等の以上の SBOM 作成に必要な情報を保持するため、SBOM 作成可能と判断し、ティア 1 同様の項目を対象とした。
- ECU ベンダー、ECU ソフトウェアサプライヤー（受託開発）共に、間接利用部品については、誤検知の精査を完全に行うことは難しいため、技術的なフィージビリティを考慮して部分適用とした。
- (e3)(e4)悪用可能性・深刻度の評価については、情報提供が十分に進んでおらず、部分適用とした。

以上のような考え方をベースに、技術的、コスト的なフィージビリティを考慮して整理した SBOM 対応モデル（案）は以下のとおりである。

表 8-4 実証を通じて検討した自動車分野における SBOM 対応モデル（参考例）

適用主体	作成範囲	生成方法	生成項目	活用法
ECU ベンダー（第 1 者）	（b1）直接利用部品	（c1）手動で特定（構成管理情報利用）・ツールで生成	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記の一部のみ	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c2）ツールで特定・生成・誤検知精査なし	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c3）ツールで特定・生成・誤検知精査あり	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価

適用主体	作成範囲	生成方法	生成項目	活用法
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
	（b2）間接利用部品	（c1）手動で特定（構成管理情報利用）・ツールで生成	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c2）ツールで特定・生成・誤検知精査なし	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定

適用主体	作成範囲	生成方法	生成項目	活用法
				（e3）（e4）悪用可能性・深刻度の評価
		（c3）ツールで特定・生成・誤検知精査あり	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
ECU ソフトウェアサプライヤー（受託開発）（第２者）	（b1）直接利用部品	（c1）手動で特定（構成管理情報利用）・ツールで生成	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c2）ツールで特定・生成・誤検知精査なし	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価

適用主体	作成範囲	生成方法	生成項目	活用法
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c3）ツールで特定・生成・誤検知精査あり	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
	（b2）間接利用部品	（c1）手動で特定（構成管理情報利用）・ツールで生成	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定

適用主体	作成範囲	生成方法	生成項目	活用法
				（e3）（e4）悪用可能性・深刻度の評価
		（c2）ツールで特定・生成・誤検知精査なし	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
		（c3）ツールで特定・生成・誤検知精査あり	（d1）標準フォーマット（SPDX、SPDX Lite 等）	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d2）大統領令最小要素を含む	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
			（d3）上記を満たさない要素	（e1）（e2）脆弱性・ライセンスの特定
				（e3）（e4）悪用可能性・深刻度の評価
(a3)サプライヤー(サードパーテ	(b1)開発者自身		(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	生成方法	生成項目	活用法
ィ)取引契約なし （第３者）		(c1)手動で特定(構成管理情報利用)・ツールで生成	(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定

適用主体	作成範囲	生成方法	生成項目	活用法
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)開発者以外(調達者、利用者)	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	生成方法	生成項目	活用法
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

8.4.3. 活用法と留意点等

前節までに示したとおり、自動車分野では型式認証における保安基準において要求される国際協定規則 UNR-155 から参照される国際標準 ISO/SAE 21434 の要求事項の例示としてソフトウェアの構成管理が挙げられている。SBOM はその効率的な手段として活用されることが期待される。SBOM 対応モデルは、その際の対応項目の具体的な推奨範囲を示すものとして活用することができる。実証において整理した SBOM 対応モデル（案）は、自動車分野の企業によるニーズや技術的なフィージビリティを考慮して整理した推奨範囲のたたき台としての例を示したものである。

このような例も参考にしつつ、今後は、自動車業界のステークホルダー（規制当局、審査機関、自動車メーカー、サプライヤー等）によりSBOM 対応モデルの検討を行い、業界でコンセンサスを形成することが期待される。それにより SBOM を活用した構成管理の具体的な推奨範囲を示すことで、自動車業界における構成管理・脆弱性管理を促進するために活用することが期待される。

8.5. SBOM 対応モデルの参考例（ソフトウェア製品分野）

分野ごとの SBOM 対応モデルの章では、SBOM に係る法制度・基準の概要、実証に基づき整理した SBOM 対応モデル（案）、活用における留意点についてまとめる。

8.5.1. 前提条件等の概要

米国大統領令に基づき、連邦政府のソフトウェア調達において SBOM を開示等することが義務化される見通しである。米国では、2021 年 5 月の大統領令後、SBOM に関する内容を含んだ複数のガイダンス等の文書が公開された。

大統領令では、2022 年 5 月 12 日までに、これらの内容を踏まえた政府調達に関する勧告を FAR 審議会に対して実施するよう、DHS に指示した。そして、この勧告を踏まえ、2023 年 10 月に FAR の改正案が発表[48]された。FAR 改正案では、連邦政府が調達する ICT 製品・サービス（例：通信サービス、電子メディア、IoT デバイス、運用技術）の請負業者に対して、SBOM の作成・維持や SBOM への政府機関のアクセスの許可を求める内容が含まれている。FAR 改正案に対する意見公募は 2024 年 2 月まで行われ、今後、正式版として発表される予定である。

[48] Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

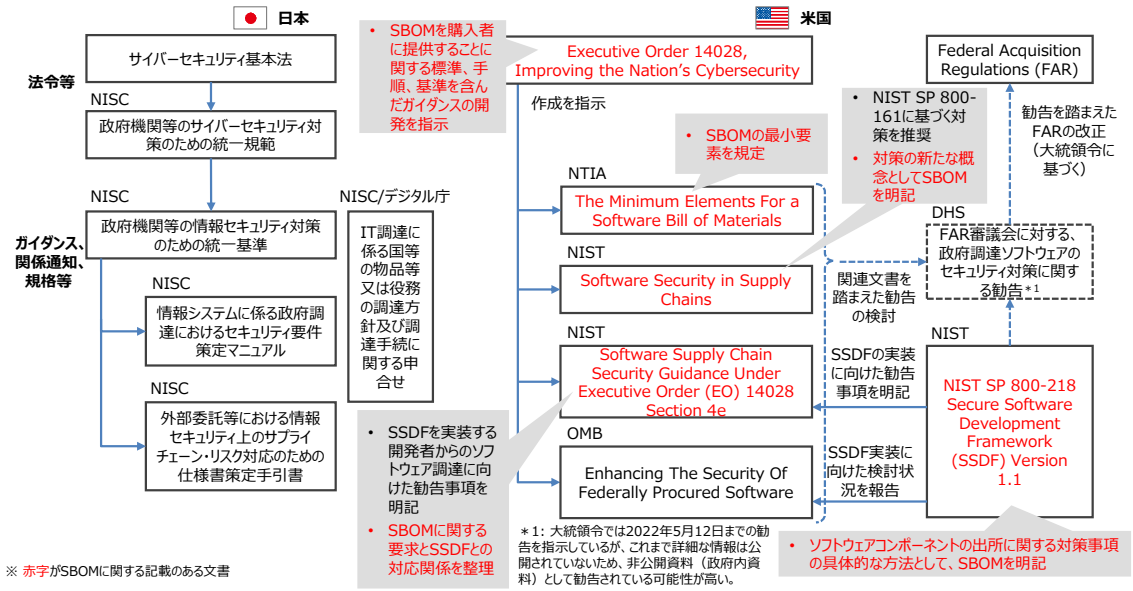

図 8-6 ソフトウェア製品分野の SBOM に係る法制度の関係整理

米国の政府調達要件は、米国政府に納入する日本企業も影響を受ける。また、国際整合の観点から日本政府や他国においても政府調達要件として、SBOM に関する要求を含める可能性があるため、SBOM への対応は重要と考えられる。

8.5.2. 実証に基づき整理した対応モデル（案）

ソフトウェア製品分野では、セキュリティ・ソフトウェア企業を例に、経済産業省 2022 年度 SBOM 実証において、以下のような点に基づき SBOM 対応モデル（参考例）について整理した。ここでは実証の対象となったサプライヤーである実証企業及びソフトウェアサプライヤー（受託開発）を対象として、ソフトウェア製品分野で求められる構成管理や技術的フィージビリティを考慮して SBOM 対応モデル（案）を整理した。

SBOM 対応モデル（案）の整理における考え方の要点は以下のとおりである。

- SBOM 生成方法の「(c2) ツールで特定・生成・誤検知精査なし」において、特に脆弱性特定でツールによる作業効率化が見込まれ、実証企業のセキュリティポリシー上、SBOM 作成・活用は開発プロセスの一部としてすでに取り入れられていることから適用可能とした。
- 「（e3）（e4）悪用可能性・深刻度の評価」に関しては、SBOM に含められる有用な情報が現状ではほぼ得られず、手動による確認、SBOM と外部情報を組合せることで可能になることから、部分適用とした。
- 「(c3) ツールで特定・生成・誤検知精査あり」について、直接利用部品は、開発チームが自覚的にコンポーネントを利用するため、正しい直接部品のリストと突き合わせる確認できるため部分適用

とした。一方、間接利用部品においては、比較すべき「正しい」情報を確かめる効率的な方法がなく、精査を行うには時間と労力がかかることからフィージビリティを考慮し、適用困難とした。

- ツールで検出した部品の精査については、誤検知と未検出それぞれの可能性があることを考慮した。
- ソフトウェア構成分析ツール（有償）を用いた部品の特定、SBOM の生成を前提に対応範囲を特定した。

以上のような考え方をベースに、技術的、コスト的なフィージビリティを考慮して整理した SBOM 対応モデル（案）は以下のとおりである。

表 8-5 実証を通じて検討したソフトウェア製品分野における SBOM 対応モデル（参考例）

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
最終ベンダー	(b1)直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
(a2)サプライヤー(開発委託先)取引契約あり	(b1)直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
(a3)サプライヤー(サードパーティ)取引契約なし	(b1)開発者自身	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
	(b2)開発者以外(調達者、利用者)	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDX Lite 等)	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

8.5.3. 活用法と留意点等

ソフトウェア製品分野は、重要インフラ分野において調達されるソフトウェアや、個人のエンターテイメント分野のアプリなど様々な種類のソフトウェアが存在する。現在のところ、米国の連邦政府機関に対する調達基準としての SSDF において SBOM を要求する例はあるが、具体的に SBOM の対応範囲まで規定するものは確認できない。

そのようなことからソフトウェア製品分野のうち強制基準が存在しない多くの分野においては、ソフトウェアの受発注者間において SBOM 対応範囲の表示と確認の慣行を普及させることで、当該分野のリスクに応じた SBOM 対応範囲へと自律的に対応が促進されることが期待できる。取引において SBOM 対応範囲を表示・確認することが普及すれば、調達者にとっては、調達するソフトウェアの構成管理・脆弱性管理のレベルを把握することができ、脆弱性リスクを抑えることが可能になる。また、供給者にとっては、SBOM 対応範囲のレベルの高さに応じて、脆弱性管理レベルの高さを示すことが可能になり、製品の価値を高めることにつながる。このような効果を通じて、SBOM 対応範囲について強制的な基準として要件化せずとも、取引における受発注者間で SBOM 対応範囲の表示と確認を一般化させることで、分野のリスクに応じて必要な SBOM 対応範囲へと調整が進むことが期待できる。

8.6. SBOM 対応モデルの参考例（医療機器分野）

医療機器分野における SBOM に係る法制度・基準の概要、実証に基づき整理した SBOM 対応モデル（案）、活用における留意点についてまとめる。

8.6.1. 法制度・基準の概要

医療機器分野においては、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（以下、「薬機法」という。）に基づいて、医療機器の製造、販売、審査・認証、市販後の安全対策にわたって一貫した規制が行われている。薬機法第 41 条第 3 項には、厚生労働大臣は、医療機器、再生医療等製品又は体外診断用医薬品の性状、品質及び性能の適正を図るため、薬事・食品衛生審議会の意見を聴き、必要な基準を設けることができるとされている[49]。

医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準（平成 17 年厚生労働省告示第 122 号）[50]

---

[49] 薬機法：https://elaws.e-gov.go.jp/document?lawid=335AC0000000145

[50] 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準：https://www.mhlw.go.jp/web/t_doc?dataId=81aa6953&dataType=0&pageNo=1

（以下、「基本要件基準[51]」という。）では、すべての医療機器又は体外診断用医薬品が具備すべき品質、有効性及び安全性に係る基本的要件を規定している。

基本要件基準第 12 条第 2 項の規定（プログラムを用いた医療機器に対する配慮）では、構成管理の要件が示されており、適合を示すために用いられる規格として JIS T 2304 が示されている[52]。さらに、令和 5 年 3 月 9 日に厚生労働省告示第 67 号「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件[53]」が官報に掲載され一部改正が公布された。これにより薬機法における基本要件基準第 12 条第 3 項にサイバーセキュリティ要件が明示された。International Medical Device Regulators Forum：国際医療機器規制当局フォーラム（以下、「IMDRF」という。）において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、2020 年 4 月に IMDRF ガイダンスが発行されており、国際整合の一環として日本国内においても IMDRF ガイダンスの内容を薬機法規制に取り入れる方向である。また、今般、「IMDRF/CYBER WG/N73FINAL:2023 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity（以下、IMDRF 追補 SBOM ガイダンス）」及び「IMDRF/CYBER WG/N70FINAL:2023 Principles and Practices for the Cybersecurity of Legacy Medical Devices（以下、IMDRF 追補レガシー医療機器ガイダンス）」の 2 つの追補ガイダンスが発出された。この 2 つの追補ガイダンスの内容に基づいて、一般社団法人日本医療機器産業連合会（以下、「医機連」という。）の医療機器サイバーセキュリティ対応ワーキンググループにおいて、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等を検討され、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書（第 2 版）（以下、「医療機器製販業者向け手引書」という。）が取りまとめられた。また、新たに医療機関における医療機器のサイバーセキュリティ確保に必要な取組、運用体制等を検討され、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」が取りまとめられた。国内における動向については、「我が国における医療機器サイバーセキュリティの規制の動向と今後の課題について[54]」を参考とし、最新の動向を調査した。

市販前のセキュリティに関わる規制（承認審査を含む）を整理し、 IMDRF ガイダンス国内導入に向けた検討、法改正等の動向について確認した事項を追記し、以下の図に示す。

---

[51] 独立行政法人医薬品・医療機器総合機構「基本要件基準とは」https://www.pmda.go.jp/files/000240068.pdf

[52] 薬生機審発 0517 第 1 号平成 29 年 5 月 17 日 厚生労働省医薬・生活衛生局医療機器審査管理課長通知 https://www.std.pmda.go.jp/stdDB/Data/RefStd/Std_etc/H290517_0517-01_01.pdf

[53] 令和 5 年 3 月 9 日官報本紙（第 933 号）https://kanpou.npb.go.jp/20230309/20230309h00933/20230309h009330003f.html

[54] 医療機器学 Vol. 90, No. 6（2020）「我が国における医療機器サイバーセキュリティの規制の動向と今後の課題について」https://www.jstage.jst.go.jp/article/jjmi/90/6/90_534/_article/-char/ja/

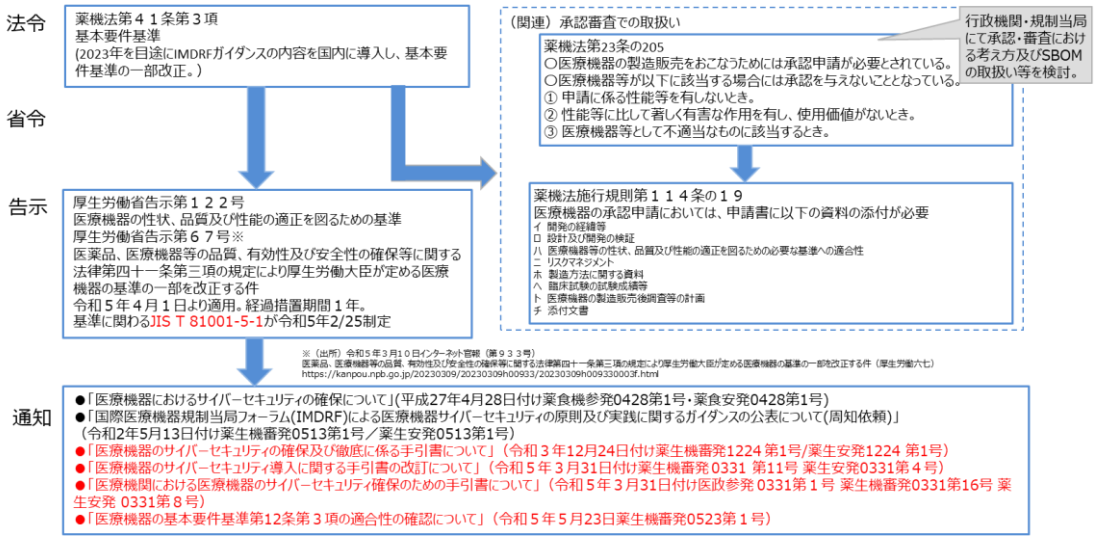

図 8-7 医療機器の市販前のセキュリティに関わる規制の概要

（出所）「我が国における医療機器サイバーセキュリティの規制の動向と今後の課題について」医機学 Vol. 90, No. 6（2020）「図１ 医薬品医療機器等法における医療機器のサイバーセキュリティに係る市販前の要求事項」を参照し、一部加筆

また、医療機器市販後のセキュリティに関わる規制を整理し、IMDRF ガイダンス国内導入に向けた検討内容について確認した事項を追記した。市販後の安全対策について、以下図に示す。

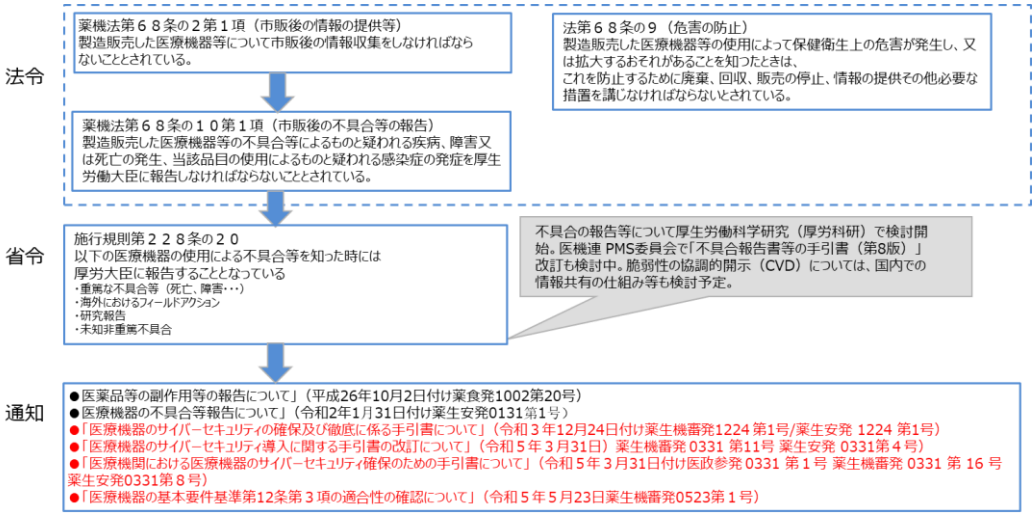

図 8-8 医療機器の市販後のセキュリティに関わる規制の概要[55]

（出所）「我が国における医療機器サイバーセキュリティの規制の動向と今後の課題について」医機学 Vol. 90, No. 6（2020）「図２ 医薬品医療機器等法における医療機器のサイバーセキュリティに係る市販後の要求事項」を参照し、一部加筆

医療機器分野では、医療機器製造販売業者（以下「医療機器製販業者」）には薬機法におけ

[55] 市販後のサイバーセキュリティの考え方について「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について（令和６年１月 15 日付け医薬安発 0115 第２号）」も発行されている。

る基本要件基準第 12 条第 2 項で構成管理がすでに義務化されており、JIS T 2304 により適合性の確認をすることができる。第 12 条第 3 項が新設され、サイバーセキュリティ要件が明確化された。第 12 条第 3 項項に関わる規格 JIS T 81001-5-1 が制定されており、医療機器に組み込むソフトウェアを含むヘルスソフトウェアのためのプロセス規格であり、製造業者が開発ライフサイクルの一部として行うアクティビティを規定している。基本要件基準第 12 条第 3 項の適合性の確認に用いることができる。

SBOM は、JIST81001-5-1、 IEC81001-5-1 (制御分野の IEC 62443-4-1 を元にした医療機器分野の規格) では要求されないが、IEC TR 60601-4-5(制御分野の IEC62443-4-2 を元にした医療機器分野の規格) では要求される顧客向け文書である。SBOM によって、顧客は、セキュリティに関連するリスク環境を監視し、セキュリティに関連するリスクについて製造業者と情報交換することが可能になるとされている。情報交換の例としては、SBOM にリストされているソフトウェアに関するセキュリティパッチについてのものがある。

8.6.2. 実証に基づき整理した対応モデル（案）

医療機器分野では、薬機法サイバーセキュリティ要件の適合性を確認するための規格 JIS T 81001-5-1 が制定されている。さらに前述のとおり、IMDRF ガイダンス、IMDRF 追補 SBOM ガイダンスに基づいて医療機器製販業者向け手引書、医療機関向け手引書が策定されている。医療機器製販業者向け手引書では、製品のライフサイクル全体を通じてリスクマネジメントが求められている。IMDRF ガイダンス等では Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等について示されている。

経済産業省 2022 年度 SBOM 実証においては、以下のような点に基づき SBOM 対応モデル（参考例）について整理した。ここでは実証の対象となった医療機器製販業者であるティア 1 開発委託先を対象として、医療機器分野で求められる構成管理や技術的なフィージビリティを考慮して SBOM 対応モデル（案）を整理した。

SBOM 対応モデル（案）の整理における考え方の要点は以下のとおりである。実証結果については、事例依存となることに留意したい。

なお、SBOM 対応モデル（案）は、JIS T 2304 において要求されているライフサイクルを通じての構成管理、JIS T 81001-5-1 のヘルスソフトウェア及びヘルス IT システムの安全、有効性及びセキュリティを実現するため、SBOM を手段の一つとして用いる場合、少なくともそれらの選択肢要素に対する説明責任が果たせているか確認する際に参考にすることができる。

- SBOM 生成・共有の作成主体「(a1)自社、(a2)サプライヤー（開発委託先）取引契約あり」では、作成範囲については医療機器製販業者が医療機器の認証範囲、SBOM 作成の対象範囲を明確に特定することにより適用可能とした。開発委託先には、契約において SBOM 提示を求める必要がある。

- SBOM 生成・共有の作成主体「(a3)サプライヤー（サードパーティ）取引契約なし」においては、一部のサードパーティは、SBOM 提供を受けて医療機器製販業者によって検証することできるため一部適用とした。ただし、IMDRF 追補 SBOM ガイダンスの 8 要素を満たさない場合がある。また、SBOM 提示されないこともあり、その SBOM の精査は困難である。
- SBOM 作成・共有の作成範囲「(b1)直接利用部品（開発主体が直接利用する部品）」については、医療機器の認証範囲を特定することにより、開発委託先のベンダーに開発者が直接利用する部品を構成ファイル等から特定し、ツール等で SBOM を生成することが可能であるため、適用可能である。
- SBOM 作成・共有の作成範囲「(b2)間接利用部品」の特定については、ツール使用によるソースコード解析、バイナリ解析、スニペット解析で部品を検出後、手動で検出した部品を合わせることによって検出漏れを極力なくすことができる。そのためツールと手動の精査の併用が望ましい。精査は可能であるがレベルについては検討が必要である。
- SBOM 活用の「(e2)脆弱性の深刻度評価」については、ツールによる CVSS 値の評価を対象として適用可能とした。「(e3)脆弱性の悪用可能性等の評価と対処」については、VEX 情報等を用いて悪用可能性、脆弱性対処の必要性を評価する。必要に応じて対処策等のアドバイザリーを発行する必要があり、十分な評価が難しいため、実証では適用不可であった。
- 実証においては SBOM を活用した脆弱性マネジメント、対処フロー検討を行った。SBOM 活用の医療機器製販業者である「(f2)最終製品ベンダー」が、医療機関等の利用者に脆弱性の発見を通知するとともに、直接開発者への修正依頼、修正後のビルド・利用者への提供を行う。必要に応じて行政機関・規制当局、ISAC 等に報告するプロセスについて机上検討できたので適用可能とした。ただし、実施するための知識の蓄積が少なく人材、資金の確保が難しいこともあり、実際の対応が難しいと判断された。

表 8-3 実証を通じて検討した医療機器分野における SBOM 対応モデル（参考例）

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
(a1)自社	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDX Lite 等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite 等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite 等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)間接利用部品		(d1)標準フォーマット（SPDX、SPDX Lite 等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
		(c1)手動で特定（構成管理情報利用）・ツールで生成	(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
(a2)サプライヤー（開発委託先）取引契約あり	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)間接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
(a3)サプライヤー（サードパーティ）取引契約なし	(b1)開発者自身	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

適用主体	作成範囲	検出・生成・検査手段	生成項目	活用法
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
	(b2)開発者以外（調達者、利用者）	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDX Lite等）	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定
				(e3)(e4)悪用可能性・深刻度の評価

8.6.3. 活用法と留意点等

医療機器分野の SBOM 対応モデル（案）は、医療機器分野の実証実施者によるニーズや技術的なフィージビリティ確認、業界団体である医機連による国内規制を踏まえた助言に基づく参考例を提示すものである。医療機器分野の実証では、IMDRF ガイダンス、IMDRF 追補ガイダンスに基づいた手引書が手法として示されているため、この内容に従っている。

8.7. SBOM 対応モデル（案）の分野横断比較

SBOM 対応項目選択肢について、実証を通じて評価検討を行い改訂した SBOM 対応モデル案の分野横断的な比較について整理し、以下に示す。

いずれの分野も OSS を含むサードパーティからの SBOM 取得は困難であるため、委託開発企業又はツールでの対応が考えられる。医療機器は、委託開発先も含めて SBOM 生成・共有し、製造販売業者が一切の責任を持つこととされている。顧客である医療機関等より SBOM 提示が求められる場合は SBOM を提示しリスクコミュニケーションを図ることが求められる。

医療機器分野においては、法的に構成管理が要件化されているため、間接利用部品を含めて説明責任を果たすことが考えられる。OSS の間接利用部品の完全な特定は技術的な課題があるため、ソフトウェア製品分野については部分的な対応としている。

図 8-9 SBOM 対応モデル（案）の分野横断的な比較

9. 付録：SBOM 取引モデル

9.1. 背景と目的（問題認識）

サプライチェーンを通じたソフトウェア部品の受発注においては、SBOM を作成しそのコストを負担する側と、SBOM を取得し脆弱性管理を効率化することにより便益が得られる側が存在することから、立場によって負担するコストと得られる便益に非対称性（偏り）が存在する。このようなことから SBOM の普及促進には、SBOM の導入方法や手順を示すだけではなく、取引契約を通じて、SBOM による便益が得られる調達者から SBOM 作成のコストを負担する供給者に対して対価が支払われなければ、SBOM は適正なレベルまで普及しないことが想定される。そのため、取引契約において SBOM に対する要求や責任を明確にして、それに応じた対価の支払いを規定することが重要になる。

本章は、SBOM に関する受発注者間のコスト負担と便益享受の非対称性を解消し、SBOM の普及促進を図るため、取引契約において規定すべき SBOM に関する要求や責任、コスト負担に関する事項について整理するものである。

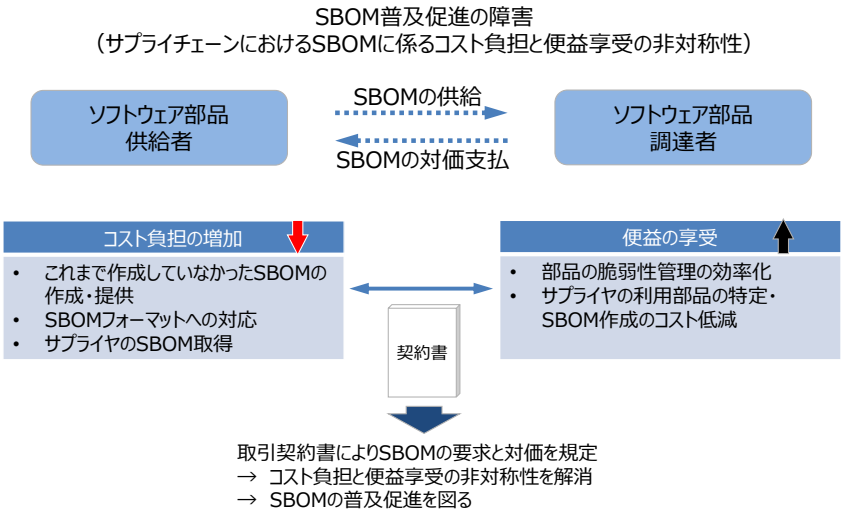

図 9-1 SBOM 普及促進の障害

9.2. 概要

9.2.1. SBOM 取引モデルとは

SBOM 取引モデルとは、ソフトウェアの受発注者間において、取引契約書において、SBOM に関する要求、責任、コスト負担に関して規定すべき主な事項について参考例を示すものであり、各企業が、それらの参考例を基に各社の契約条項を作成するもとになる考え方を示すものである。

9.2.2. 対象読者

本章は、ソフトウェアの受発注者における SBOM に関する要求、責任、コスト負担等の規定を定める取引契約に係る法務担当者、開発者を主な想定読者とする。

9.2.3. 本章の構成

本章の以下の構成は次のとおりである。9.3 取引モデルの考え方では、SBOM 取引モデルの意義、活用の考え方を示す。9.4 SBOM 取引モデルでは、取引モデルの構成、規定すべき事項についてまとめる。9.5 では、SBOM 対応モデルと SBOM 取引モデルの関係とについてまとめる。9.6 では、既存のソフトウェア開発に関わるモデル契約書と本章の SBOM 取引モデルの関係について示す。9.7 では、取引モデルの活用パターンとステップを示す。9.8 では、本章の取引モデルのステータスと今後の期待される改訂について示す。

9.3. 取引モデルの考え方

SBOM のメリットは、サプライチェーンを通じて標準化された部品情報の共有と自動処理による効率化が挙げられる。特に SBOM を受け取る委託元の便益は大きいが、委託先はそのために追加負担を強いられることもあり、受発注者間で得られる便益が異なる。

そのようなことから、サプライチェーンを通じた SBOM の普及のためには、受発注者間で得られる便益に応じた対価負担の取決めが必要であり、委託契約において、SBOM の対応範囲とそれに対する対価負担、責任の明確化が必要である。

SBOM 取引モデルは、そのような SBOM に対する要求事項と派生する対価負担、責任関係について取決事項を示すものである。SBOM 取引モデルは各社ごとの契約書作成において参考となり、SBOM の効果的な利活用に資するものである。

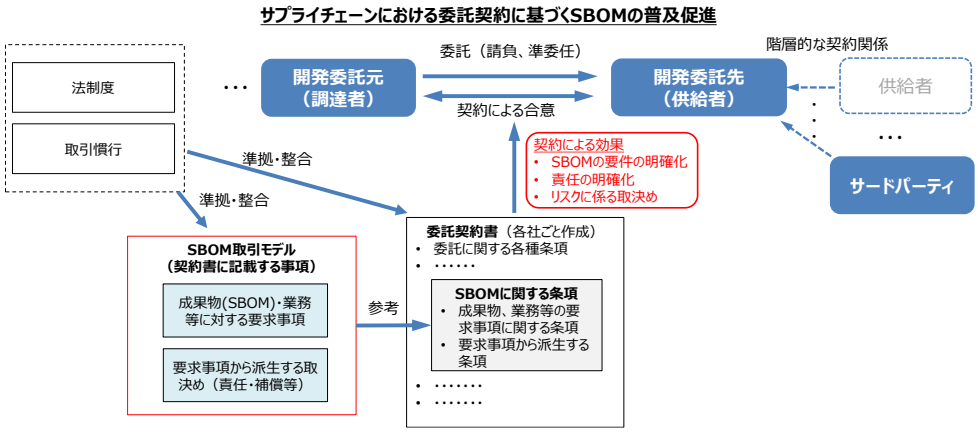

図 9-2 SBOM 取引モデルを活用した SBOM 普及促進の考え方

取引モデルは、直接的には、委託開発契約のある企業との関係を規定するが、間接的に、サードパーティ部品の SBOM のカバー範囲に対する要件も規定することができる。例えば、SBOM 作成範囲として、委託開発先やサードパーティ（商用既製品、OSS）を対象とするかどうかや、再利用部品を対象とするかどうかによってサードパーティ部品のカバー範囲を規定することができる。

9.4. SBOM 取引モデル

9.4.1. 取引モデルの構成

SBOM 取引モデルは、開発委託契約書及び発注仕様書において SBOM に関して規定すべき主な事項を示すものである。実際の条項については、法的な明確性を確保するように作成する必要はあるが、本章では、即時性を重視し、項目レベルで重要な要素を網羅するように整理した。

取引モデルの構成については、SBOM 対応モデルをベースとして、SBOM 自体に対する要求事項と、IPA、JEITA などから公開されるソフトウェア開発に関するモデル契約書の責任と保証に関わる項目を含めるとともに、本取引モデルで重視する SBOM のコスト負担、権利・機密保持などを主な要素とし、以下の構成として整理した。

区分		概要
SBOM 要求事項	フォーマット・標準	SBOM のフォーマットや標準に関する要求事項を定める。
	品質・信頼性	SBOM 対応モデルにおける SBOM の品質に相当する要求事項を定める。
	保守・運用	SBOM 対応モデルにおける脆弱性管理等に関する要求事項を定める。
責任と保証		SBOM に関する責任、損害賠償などについて定める。
コスト負担		SBOM 作成・管理に関わる妥当なコスト負担を実現するための事項を定める。
権利・機密保持		SBOM の知的財産権、関連する機密保持に関する事項を定める。

これらの要素については、経済産業省 SBOM 実証事業を通じて得られた分野ごとの前提条件（付録の法制度、取引慣行、開発環境）を考慮して整理した。次節に、これらの構成要素ごとに検討した SBOM 取引モデルの規定事項を示す。

9.4.2. 委託契約において規定すべき事項（案）

前節の SBOM 取引モデル構成案に対して、SBOM 対応モデルの選択肢及び実証における前提条

件（付録の法制度、取引慣行、開発環境）に基づき、委託契約書において規定すべき主な事項を整理したものを示す。これらの項目は、経済産業省ソフトウェアタスクフォースにおける意見に基づき改訂を行ったものである。

表 9-1 SBOM 取引モデル（開発委託契約で規定すべき事項）

区分		規定すべき事項	レベル
SBOM要求事項	フォーマット・標準	**（SBOMフォーマット）※1** 採用するSBOM標準フォーマットについて規定する。（SPDX, CycloneDX, SWID等の標準とバージョンを規定）	基礎
		（ID標準）※1 採用する部品ID標準を規定する。（CPE, PURL, SWD, 独自形式等）	基礎
		（SBOM最小要素）※1 採用するSBOMフォーマットの要素項目のうち最小要素を規定する。NTIAのSBOM最小要素を参考にする。	基礎
	品質・信頼性 （SBOM対応モデルに該当）	**（対象サプライヤ契約形態）** SBOM作成範囲として、委託開発契約、サードパーティ利用規約（商用既製品、OSS）の契約形態による範囲を規定する。	基礎
		（再帰的利用部品）※1 SBOM作成範囲として、直接利用部品か再帰的な間接利用部品までとするか規定する。	発展
		（構成解析手法の適用範囲）※1 間接利用部品について、部品を特定する際に利用する構成解析手法の適用範囲を規定する。（依存関係解析、ファイル照合、スニペット解析等）	発展
		（部品精査の要否）※1 ツールによる部品特定の結果に対して、手動による誤検知・検出漏れの精査の要否を規定する。	発展
		（部品の対象フェーズ）※1 部品情報の範囲としてビルド時、ランタイム、クラウドサービス等の範囲を規定する。	発展
		（サードパーティ部品の事前合意） サードパーティ部品（商用部品、OSS）を利用する場合、事前の申告と合意の要否について規定する。	基礎
	保守・運用	**（共有方法）※1** SBOMファイルによる授受またはSaaS等によるリアルタイム共有について規定する。	基礎
		（VEX対応）※1 SBOMに関連する脆弱性情報について悪用可能性に基づくVEX情報の提供を行うか規定する。	発展
		（SBOM更新）※1 ソフトウェアのアップデート、SBOM不具合修正等に応じて、SBOMを更新する期限や頻度を規定する。	基礎
		（脆弱性監視・通知） ソフトウェアの運用フェーズにおいて、脆弱性を監視し、脆弱性が発見された場合に、調達者に通知の期限を規定する。	発展
		（脆弱性対応・優先付け）※1 脆弱性が発見された際に、脆弱性対応の要否、優先付け（トリアージ）について調達者に情報提供を行うか規定する。	発展
		（EOL・EOS） サードパーティ部品および委託開発部品のEOL、EOSやその期限変更に対する通知について規定する。	発展
責任と保証		**（エビデンス提出）** SBOM要求事項について適合していることを証明するエビデンス、第三者証明の提出の要否について規定する。	発展
		（契約不適合責任） SBOM要求事項に対する不適合が見つかった場合には、SBOM修正等の瑕疵対応の要否について規定する。	基礎
		（損害賠償）※2 SBOM要求事項の不適合が原因で事故が発生した場合、損害賠償額上限等について規定する。ライセンス違反の損害賠償を含む。	基礎
		（免責） SBOM要求事項への適合性エビデンスを提出している場合について、技術的制約（ツールの誤検知など）に帰する理由で、損害が発生した場合について損害賠償の制限、免責について規定する。	発展
コスト負担		**（見積）※2** SBOM要求事項、責任・保証に基づき見積の作成し、その合意金額に基づき対価支払について規定する。	基礎
権利・機密保持		**（知的財産権の帰属）** 作成したSBOMの知的財産権、使用権の帰属、第三者への提供可否について規定する。	発展
		（機密保持） SBOMの機密保持・管理およびSBOMを用いたリバースエンジニアリングの禁止について規定する。	発展

※1　発注仕様書に記載することも想定される。

※2　ソフトウェア開発一般の請負契約と共通化することが想定される。

SBOM 取引モデルにおけるこれらの規定事項は、脆弱性管理、ソフトウェア品質保証に重要な要件を言語化したものと言える。これらの規定事項は、主に要件定義後の請負契約が対象となることが想定される。

9.5. SBOM 対応モデルと SBOM 取引モデルの関係と位置づけ

SBOM 対応モデルと SBOM 取引モデルは、密接に関係しており、それぞれの目的に応じて一方又は両方を活用することにより SBOM の社会実装を進めていくことが期待できる。SBOM 対応モデルと SBOM 取引モデルの関係と位置づけを図示したものが以下の図である。

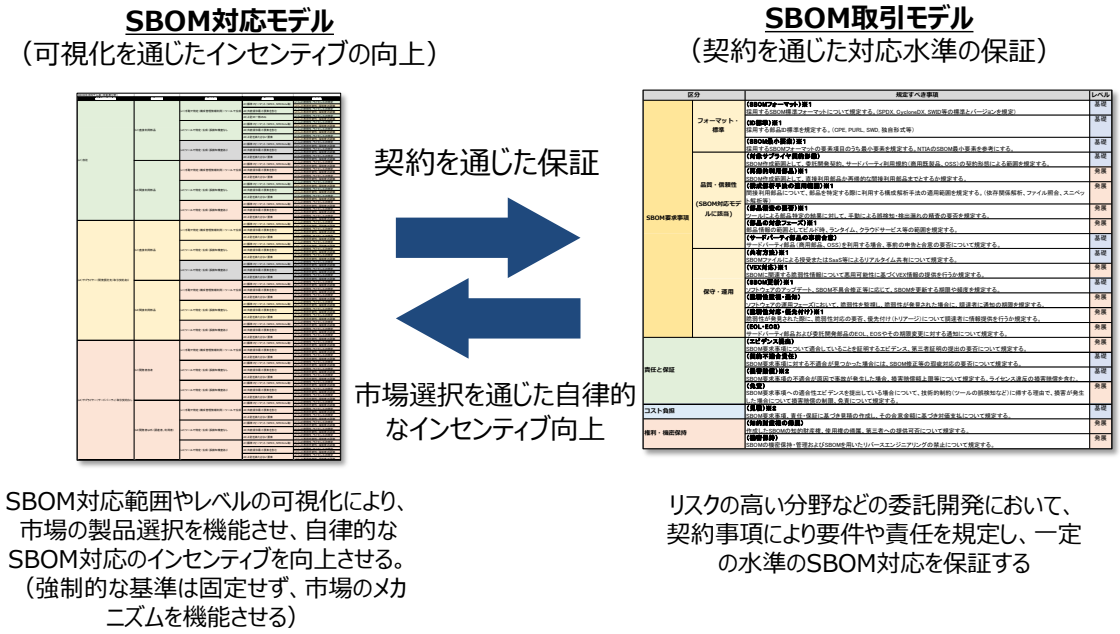

図 9-3 SBOM 対応モデルと SBOM 取引モデルの関係と位置づけ（全体像）

SBOM 対応モデルは、SBOM 対応範囲の可視化フレームワークであり、SBOM 対応範囲やレベルの可視化により、市場の製品選択を機能させ、自律的な SBOM 対応のインセンティブを向上させるための仕組みである。SBOM 対応範囲について、強制的な基準は固定せず、市場のメカニズムを機能させることで、ソフトウェア受発注の取引当事者が自律的に SBOM の対応レベルを妥当なレベルに向上させる仕組みである。

一方、SBOM 取引モデルは、契約を通じて SBOM 対応水準を確実なものとなるように保証するものである。リスクの高い分野などの委託開発において、契約事項により要件や責任を規定し、一定の水準の SBOM 対応を保証することが目的である。このように契約条項により発注者と受注者が合意することによって SBOM の社会実装を進めるものである。

9.6. 既存のモデル契約書との関係

ソフトウェアのモデル契約書はソフトウェアの品質を確保し、受発注者間の認識のズレを解消し、ソフトウェア開発におけるトラブルを解消する上で重要な役割を果たす。代表的なモデル契約書としては以下の２つが挙げられる。

- **情報処理推進機構「情報システム・モデル取引・契約書（第２版）」**

情報システムの信頼性の向上・取引可視化に資する理想的な取引・契約モデルを示すもの。

- **電子情報技術産業協会「JEITA ソフトウェア開発モデル契約の解説」**

ソフトウェア開発取引の適正化、情報システムの信頼性向上という観点をも踏まえて、ユーザーとベンダーの協力、仕様、役割分担、必要な時期に確定すべき課題等に関する双方の認識を合わせるための契約条件について具体化させていくもの。

これらのモデル契約書は、ソフトウェア開発における契約書について条項レベルで網羅に示した雛形と解説を示している。これらの既存のモデル契約書には、SBOM に関する条項は規定されていないため、SBOM 取引モデルは、それらを補うものとして活用することができる。ただし、SBOM 取引モデルは、即時性を優先して公開するため、契約書の条項レベルの雛形ではなく、規定すべき重要な事項レベルでの参考例を示すものである。

9.7. 活用パターン

SBOM 取引モデルの活用パターンは以下の二通りが想定される。

1. <u>自社のソフトウェア開発契約書ベース</u>

自社のソフトウェア開発契約書雛形又は既存の契約書例をベースに、SBOM 取引モデルの規定事項を反映し契約書を完成させる。

(1) SBOM 取引モデルの規定事項の採否判断

取引モデルに挙げる規定事項のうち、自社のリスクや要求水準に基づき、採用する事項を選定する。

(2) SBOM 取引モデルとのマッピング

自社契約書雛形の構成に基づき、選択した取引モデル規定事項の該当箇所を特定する。

(3) 自社契約書に対応して取引モデルの条項文作成

自社契約書における取引モデル規定事項の位置づけや影響を考慮して、規定事項について、条項文案を作成する。

(4) 取引相手との協議

契約書にSBOM 取引モデルを反映した契約書案について取引相手と協議・合意を図りSBOM

取引モデルを含む契約書を完成させる。

2. **既存のソフトウェア開発モデル契約書ベース**

IPA や JEITA の既存のソフトウェア開発モデル契約書をベースに、SBOM 取引モデルの規定事項を反映し、契約書を完成させる。

(1) SBOM 取引モデルの規定事項の採否判断

取引モデルに挙げる規定事項のうち、自社のリスクや要求水準に基づき、採用する事項を選定する。

(2) SBOM 取引モデルとのマッピング

ソフトウェア開発モデル契約書の構成に基づき、選択した取引モデル規定事項の該当箇所を特定する。

(3) 自社契約書に対応して取引モデルの条項文作成

ソフトウェア開発モデル契約書における取引モデル規定事項の位置づけや影響を考慮して、規定事項について、条項文案を作成する。

(4) 取引相手との協議

契約書に SBOM 取引モデルを反映した契約書案について取引相手と協議・合意を図り SBOM 取引モデルを含む契約書を完成させる。

以上のような活用パターンを選択し、選択した活用パターンのステップに基づき SBOM 取引モデルに対応した契約書を作成する。

9.8. 課題と今後の検討の方向性

SBOM 取引モデルは、即時性を優先して公開するものであり、以下に挙げる課題が存在する。今後、これらの課題を解決することで、導入しやすい形式に改訂することが期待される。

- **取引モデルの規定事項の契約書条項化**

  SBOM 取引モデルは、契約書条項まで示しておらず、契約書において規定すべき重要な事項レベルの規定事項を整理したものである。実際の契約書作成においては、法的な明確性を確保した条項文案を示すことで、利用しやすい取引モデルとすることができる。既存のソフトウェア開発一般の請負契約と、SBOM 取引モデルの条項案を、SBOM 取引モデルの利用者が一体化した上で契約書雛形として発展させることができる。

- **SBOM 取引モデルの解説書**

  SBOM 取引モデルの利用者が、ソフトウェア開発モデル契約書に SBOM 契約書条項を統合した契約書雛形を作成し、各条項に対する活用法の解説を示すことが期待される。特に、分野や要求レベルに応じた契約書条項の選択肢方法やその考え方についての解説をまとめることが期待される。

- **契約書と発注仕様書の使い分け**

  SBOM 取引モデルの規定事項は、契約書に記載すべき事項と発注仕様書に記載すべき事項に

分解することができる。請負契約、準委任契約に応じて、そのような文書に分解した SBOM 取引モデルの活用方法について示すことが期待される。

10.付録：チェックリスト・用語集等

10.1.　SBOM 導入に向けた実施事項チェックリスト

SBOM 導入に関する環境構築・体制整備フェーズ、SBOM 作成・共有フェーズ、SBOM 運用・管理フェーズの 3 つのフェーズにおける実施事項をチェックリストとして以下にまとめる。

表 10-1　SBOM 導入に向けた実施事項チェックリスト

フェーズ	ステップ	実施事項	チェック
環境構築・体制整備フェーズ	SBOM 適用範囲の明確化	対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する。	□
		対象ソフトウェアの正確な構成図を作成し、SBOM 適用の対象を可視化する。	□
		対象ソフトウェアの利用者及びサプライヤーとの契約形態・取引慣行を明確化する。	□
		対象ソフトウェアの SBOM に関する規制・要求事項を確認する。	□
		SBOM 導入に関する組織内の制約（体制の制約、コストの制約等）を明確化する。	□
		整理した情報に基づき、SBOM 適用範囲（5W1H）を明確化する。詳細は、8.の SBOM 対応モデルも参考とする。	□
		調達又は供給するソフトウェアについて、SBOM 取引モデルに基づき、取引相手との間で SBOM に関する要求事項、責任関係について明確にする。	□
	SBOM ツールの選定	対象ソフトウェアの開発言語や組織内の制約を考慮した SBOM ツールの選定の観点を整理する。 （選定の観点の例：機能、性能、解析可能な情報、解析可能なデータ形式、コスト、対応フォーマット、コンポーネント解析方法、サポート体制、他ツールとの連携、提供形態、ユーザーインターフェース、運用方法、対応するソフトウェア開発言語、日本語対応等）	□
		整理した観点に基づき、複数の SBOM ツールを評価し、選定する。	□

フェーズ	ステップ	実施事項	チェック
	SBOM ツールの導入・設定	SBOM ツールが導入可能な環境の要件を確認し、整備する。SBOM 対応モデルで特定した対応範囲を満たすようにツール機能や手動による対応の組合せを考える。	□
		ツールの取扱説明書や README ファイルを確認して、SBOM ツールの導入・設定を行う。	□
	SBOM ツールに関する学習	ツールの取扱説明書や README ファイルを確認して、SBOM ツールの使い方を習得する。	□
		ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。	□
SBOM 作成・共有フェーズ	コンポーネントの解析	SBOM ツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析する。	□
		SBOM ツールの解析ログ等を調査し、エラー発生や情報不足による解析の中断や省略がなく、解析が正しく実行されたかを確認する。	□
		コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れがないかを確認する。	□
	SBOM の作成	作成する SBOM の項目、フォーマット、出力ファイル形式等の SBOM に関する要件を決定する。	□
		SBOM ツールを用いて、当該要件を満足する SBOM を作成する。	□
		SBOM 作成においては、サプライチェーンを通じて、誰が、何を、どこまで実施するかについて明確にし、取引者間で合意する。8 章付録を参考とする。	□
	SBOM の共有	対象ソフトウェアの利用者及び納入先に対する SBOM の共有方法を検討した上で、必要に応じて、SBOM を共有する。	□
		SBOM の共有に当たって、SBOM データの改ざん防止のための電子署名技術等の活用を検討する。	□
SBOM 運用・管理フェーズ	SBOM に基づく脆弱性管理、ライセンス管理等の実施	脆弱性に関する SBOM ツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。	□

フェーズ	ステップ	実施事項	チェック
		脆弱性情報の特定においては、①SBOM 既成ツールの利用②脆弱性 DB の API を利用したスクリプト③脆弱性 DB の WebUI などの活用を考慮し、適切な方法を選択する。（7.4.1 を参考とする。）	□
		脆弱性優先付けにおいては、脆弱性対応要否の簡易なフィルタリング、脆弱性のインシデント有無、Exploit コードの公開有無、VEX 情報の活用、CVSS スコアなどに基づき費用対効果を考慮して優先付けを行う。優先付けにおいては、SSVC の考え方を参考に必要に応じて優先度のカテゴリー分類を行う。（7.4.2 を参考とする。）	□
		脆弱性情報の共有において、脆弱性対応の優先付けに必要になる付加情報など共有情報の特定、サプライチェーン上の共有相手の特定、共有手段の特定を行い、必要性に応じた情報共有を行う。（7.4.3 を参考とする。）	□
		脆弱性に対応においては、脆弱性の修正を伴わない初動対応と、脆弱性の修正を伴う根本対応について実施する。（7.4.4 を参考とする。）	□
		ライセンスに関する SBOM ツールの出力結果を踏まえ、OSS のライセンス違反が発生していないかを確認する。	□
	SBOM 情報の管理	作成した SBOM は、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する。	□
		SBOM に含まれる情報や SBOM 自体を適切に管理する。	□

10.2. 用語集

10.2.1. SBOM やソフトウェアに関する用語の定義

- EOL（End of Life）
  製品やサービスにおいて販売やサポートが終了し、それ以上継続して使用すべきでないとされる使用期限のこと。
- OTS（Off-The-Shelf）
  サプライヤーが一般的に利用するソフトウェアのコンポーネントであり、サプライヤーが完全なソフトウェアライフサイクル管理を主張できないコンポーネントのこと。
- OSS（Open Source Software）
  ソフトウェアのソースコードが公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェアのこと。
- SBOM（Software Bill of Materials）
  コンポーネントやそれらの依存関係の情報も含めた機械処理可能なインベントリー（一覧表）のこと。コンポーネントやその依存関係をすべて表現している場合もある。また、どこの部分が欠けているかという情報が含まれている場合もある。OSS だけではなくプロプライエタリソフトウェアに活用することもでき、広く一般に公開するほか関係者だけに提示するという使用方法も存在する。
- SBOM 作成者（SBOM Author）
  SBOM を作成するエンティティのこと。必ずしも SBOM 作成者とサプライヤーが一致しないことに留意する必要がある。SBOM 作成者とサプライヤーが異なる場合、あるエンティティが、異なるサプライヤーによって作成又は含有された構成要素について主張した場合、当該エンティティが SBOM 作成者としてみなされる。
- SBOM 利用者（SBOM Consumer）
  SBOM を入手するエンティティのこと。ほとんどのエンティティは、サプライヤーであると同時に SBOM 利用者でもあり、SBOM データを有するコンポーネントを自身のソフトウェアに使用し、そのデータを下流に渡すことが可能となる。
- SBOM 項目（SBOM Entry）
  SBOM のコンポーネントと関連する属性のこと。行列形式の SBOM の場合、行に該当する。
- SBOM システム（SBOM System）
  SBOM を作成、共有、活用、管理する能力を提供する一連の要素及びプロセスのこと。
- SBOM ツール（SBOM Tool）
  SBOM の作成、共有、活用、管理することができるツールのこと。SBOM 管理ツール、OSS 管理ツール、ソフトウェア構成解析（SCA）ツール等とも呼ばれることがあり、パッケージとして提供されるツ

ールのほか、クラウドソフトウェアとして提供されるツールも存在する。

- VEX（Vulnerability Exploitability Exchange）
  特定の製品が既知の脆弱性の影響を受けるかどうかを示すセキュリティアドバイザリーの一つの形態のこと。

- 依存関係（Dependency Relationship）
  ソフトウェア Y に、上流のコンポーネント X が含まれる関係性の特徴づけのこと。

- エンティティ（Entity）
  ソフトウェアやコンポーネントに関連する企業、団体、組織、個人のこと。

- 関係性表明（Relationship Assertion）
  ある作成者における、他サプライヤーのコンポーネントの知識の範囲のこと。Unknown、Root/None、 Partial、 Known の 4 つのカテゴリーが存在する。

- コードベース（Codebase）
  特定のソフトウェア、アプリケーション、コンポーネント等を構築するために使用されるソースコード全体のこと。

- コンポーネント（Component）
  サプライヤーによって定義されるソフトウェアの単位のこと。コンポーネントは、サプライヤーにより構築、パッケージ化又は納入される時点で定義される。ソフトウェア製品、機器、ライブラリ、単一ファイル等も一つのコンポーネントに位置づけられるほか、OS、オフィススイート、データベースシステム、自動車、自動車のエンジンコントロールユニット（ECU）、医療用画像処理装置、インストールパッケージ等のコンポーネントの集合体も、コンポーネントとなる。多くのコンポーネントがサブコンポーネントを含む。

- 再利用（Reuse）
  ソフトウェア部品を複数から利用すること。

- 再帰的利用（Recursive Use）
  ソフトウェア部品などにおいて自分自身を呼び出すことで再利用すること。本書では、サプライチェーンにおいて、繰り返しサプライヤーがつながる形で部品を再利用するケースなどにも用いる。

- 最小要素（Minimum Elements）
  米国の大統領令（Executive Order 14028）に基づき NTIA より 2021 年 7 月 12 日に発表された SBOM に含めるべき最小要素のこと。データフィールド、自動化サポート、プラクティスとプロセスの 3 つのカテゴリーに基づく具体的な定義が示されている。

- サブコンポーネント（Subcomponent）
  コンポーネントに含まれるコンポーネントのこと。

- サプライヤー（Supplier）
  コンポーネントを開発、定義及び識別するエンティティで、理想的には当該コンポーネントに関連する SBOM を作成するエンティティのこと。サプライヤーは、製造者、ベンダー、デベロッパー、システムイン

テグレーター、保守事業者、サービスプロバイダーとも呼ばれる。ほとんどのサプライヤーは SBOM の利用者でもある。上流のコンポーネントを持たないサプライヤーは、ルートエンティティとも呼ばれる。

- シンボリックリンク（Symbolic Link）
  OS のファイルシステムにおける機能の一つで、特定のファイルやディレクトリを示す別のファイルのこと。
- 推移的依存関係（Transitive Dependency）
  ソフトウェア X にコンポーネント Y が含まれ、コンポーネント Y にコンポーネント Z が含まれる場合に、ソフトウェア X にコンポーネント Z が含まれる関係性の特徴づけのこと。
- スニペット（Snippet）
  ソースコード内のコード断片のこと。
- 属性（Attribute）
  コンポーネントに関する特性や情報のこと。行列形式の SBOM の場合、列に該当する。
- ソフトウェア構成解析（SCA：Software Composition Analysis）
  狭義には、製品が利用しているコンポーネントを識別すること。一般的には、特定した各コンポーネントの脆弱性やライセンスリスクを管理することを指す。
- 中間サプライヤー（Intermediate Supplier）
  上流のコンポーネントを、下流工程として新たなコンポーネントに加工するサプライヤーのこと。多くのサプライヤーは中間サプライヤーとして扱われる。
- プライマリーコンポーネント（Primary Component）
  SBOM によって記述される対象のコンポーネントのこと。
- プロプライエタリソフトウェア（Proprietary Software）
  ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェアのこと。
- 要素（Element）
  SBOM システムの一部のこと。
- ランタイムライブラリ（Run-time Library）
  プログラムの実行時に必要なライブラリのこと。

10.2.2. サイバーセキュリティに関する用語の定義

- CVSS（Common Vulnerability Scoring System）
  FIRST（Forum of Incident Response and Security Teams）が管理する脆弱性の深刻度を同一の基準の下で定量的に比較できる評価方法のこと。0.0～10.0 の間でスコアが定まる。
- CWE（Common Weakness Enumeration）

ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準のこと。米国非営利団体 MITRE を中心として仕様策定。

- ISMS（Information Security Management System）
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組みのこと。国際規格 ISO/IEC 27001 に要求事項が定められている。
- OWASP（Open Web Application Security Project）
  Web をはじめとするソフトウェアのセキュリティ関する情報共有と普及啓発を目的とした、オープンソースソフトウェアコミュニティのこと。
- PSIRT（Product Security Incident Response Team）
  自社製品のセキュリティの向上を担い、インシデントが発生した際に対応する組織のこと。
- 脅威（Threat）
  システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因のこと。[JIS Q 27000:2014]
- 脅威情報（Threat Intelligence）
  脅威からの保護、攻撃者の活動検知、脅威への対応等に役立つ可能性のある情報のこと。[NIST SP 800-150]
- 脅威分析（Threat Analysis）
  機器やソフトウェア、システム等に対する脅威を抽出し、その影響を評価すること。主に、製品の要件定義、設計フェーズにて行われる。
- サイバー攻撃（Cyber Attack）
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試みのこと。[JIS Q 27000:2014]
- サイバーセキュリティ（Cybersecurity）
  電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。
- サプライチェーン（Supply Chain）
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れのこと。[ISO 28001:2007, NIST SP 800-53 Rev.4]
- 脆弱性（Vulnerability）
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2014]
- 認証（Authentication）

エンティティの主張する特性が正しいという保証の提供のこと。[JIS Q 27000:2014]

- 認可（Authorization）
  アクセス権限に基づいたアクセス機能の提供を含む権限の付与のこと。 [ISO 7498-2:1989]
- プロトコル（Protocol）
  複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、予め決められた約束事や手順の集合のこと。
- マルウェア（Malware）
  許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェアのこと。[NIST SP 800-53 Rev.4]
  セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。
- リスク（Risk）
  目的に対する不確かさの影響のこと。[JIS Q 27000:2014]

10.3. 参考情報

10.3.1. SBOM に関する参考文書

本項では、国内外の政府関係機関が発表している SBOM に関する参考文書を列挙する。

- **米国 NTIA : Roles and Benefits for SBOM Across the Supply Chain（2019 年 11 月）**
  ソフトウェア開発者、購入者、利用者のそれぞれの視点で、SBOM を利用することのメリットをまとめた文書。メリットは、コスト、セキュリティ、ライセンス、コンプライアンス、サプライチェーンにおけるソフトウェアの安定性ごとに整理されている。
  https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf
- **米国 NTIA : Software Bill of Materials (SBOM)（2020 年 8 月）**
  SBOM の検討背景、ソフトウェアエコシステムにおける SBOM の役割や有効性、SBOM の概要をまとめた文書。
  https://www.ntia.gov/files/ntia/publications/sbom_overview_20200818.pdf
- **米国 NTIA : SBOM FAQ（2020 年 11 月）**
  SBOM の概要、利用効果、SBOM の生成や配布等に関してまとめた FAQ 集。
  https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf
- **米国 NTIA : Sharing and Exchanging SBOMs（2021 年 2 月）**
  SBOM データがサプライチェーン上でどのように共有されるかに関するオプションを説明した文書。

SBOM データを作成したサプライヤーと SBOM の利用者の負担を最小化することを目的としている。
https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf

- **米国 NTIA : SBOM Tool Classification Taxonomy（2021 年 3 月）**
  SBOM ツールの分類を示した文書。ツールの利用目的を SBOM の作成・利用・変換の 3 つに分類し、それぞれの目的におけるツールのタイプが整理されている。
  https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf

- **米国 NTIA : Software Identification Challenges and Guidance（2021 年 3 月）**
  ソフトウェアコンポーネントを国際的に一意に識別するための課題を説明した文書。課題を解決するための対処方法・ガイダンスを示すことを目的としている。
  https://www.ntia.gov/files/ntia/publications/ntia_sbom_software_identity-2021mar30.pdf

- **米国 NTIA : SBOM at a Glance（2021 年 4 月）**
  SBOM の活用方法、ソフトウェアサプライチェーンの透明性確保において SBOM が果たす役割、参考となる文書についてまとめた文書。SBOM に含めるべき情報も整理されている。なお、JPCERT/CC によって日本語訳された文書も公開されている。
  https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf
  https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_ja.pdf（日本語版）

- **米国 NTIA : SBOM Options and Decision Points（2021 年 4 月）**
  SBOM に関して現在の手法で実現可能なことや、SBOM のサプライヤー及び利用者の間でのニーズの明確化を支援することを目的とした文書。
  https://www.ntia.gov/files/ntia/publications/sbom_options_and_decision_points_20210427-1.pdf

- **米国 NTIA : The Minimum Elements For a Software Bill of Materials (SBOM)（2021 年 7 月）**
  SBOM の最小要素を定義した文書。最小要素は 3 つのカテゴリーに分けられ、各カテゴリーの概要や SBOM に含めるべき具体的な項目が定義されている。
  https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

- **米国 NTIA : Vulnerability-Exploitability eXchange (VEX) – An Overview（2021 年 9 月）**

特定のソフトウェアコンポーネントが脆弱性の影響を受けるかどうかを判断する指標である VEX について、その概要を説明した文書。VEX は、特定の製品に存在する脆弱性の状態を表すもので、文書では 4 段階で状態を表す方針が示されている。
https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

- **米国 NTIA：How-To Guide for SBOM Generation（2021 年 10 月）**
  SBOM 生成の手引として SBOM 生成のための情報収集方法と、具体的な SBOM 生成方法の 2 つの観点をまとめた文書。本手引は、NTIA によるヘルスケア分野の SBOM PoC を通じて策定されたが、ヘルスケア分野だけでなくあらゆる業界における SBOM 生成においての活用が期待されている。
  https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf
- **米国 NTIA：Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)（初版：2019 年 11 月、改定：2021 年 10 月）**
  SBOM の概念や関連用語、ソフトウェアコンポーネントの表現に関する基本的な考え方を示すとともに、SBOM の作成プロセスを示した文書。
  https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf
- **米国 NTIA：SBOM Myths vs. Facts（2021 年 11 月）**
  SBOM のメリットを正しく示すことを目的に、SBOM に関する代表的な誤解（神話）と、その誤解を解くための事実を整理した文書。
  https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf
- **米国 NTIA：Software Suppliers Playbook: SBOM Production and Provision（2021 年 11 月）**
  ソフトウェアサプライヤーを対象とした SBOM 生成に関するプレイブック。本プレイブックでは、「SBOM 作成手順」、「SBOM 作成に当たって考慮すべき事項」及び「SBOM に関する補足事項」の 3 つの事項についてまとめられている。
  https://www.ntia.gov/files/ntia/publications/software_suppliers_sbom_production_and_provision_-_final.pdf
- **米国 NTIA：Software Consumers Playbook: SBOM Acquisition, Management, and Use（2021 年 11 月）**
  ソフトウェア利用者を対象とした SBOM 利用に関するプレイブック。本プレイブックでは、「サプライヤーから SBOM を取得する際の注意点」、「SBOM 活用のプロセス及びプラットフォーム」、「SBOM の知的財産及び機密保持」に関する注意点等がまとめられている。
  https://www.ntia.gov/files/ntia/publications/software_consumers_sbom_acqu

isition_management_and_use_-_final.pdf

- **米国 NTIA : Survey of Existing SBOM Formats and Standards - Version 2021（初版 : 2019 年、改定 : 2021 年）**
  既存の SBOM フォーマットや基準に関する調査結果や今後の課題に関して整理した文書。既存の SBOM フォーマットについては、SPDX、CycloneDX、SWID の 3 つについて、概要、ユースケース、特徴等がまとめられている。
  https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf
- **米国 NIST : SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities（2022 年 2 月）**
  ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法をまとめたフレームワーク文書。手法は 4 つのカテゴリーに分類され、各手法を実践するためのタスクが体系整理されている。
  https://csrc.nist.gov/publications/detail/sp/800-218/final
- **米国 CISA : Vulnerability Exploitability eXchange (VEX) – Use Cases（2022 年 4 月）**
  VEX ドキュメントに含めるべき最小要素を示した文書。また、VEX ドキュメントを作成するための具体的な事例としてユースケースが紹介されている。
  https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Document_508c.pdf
- **米国 CISA : Vulnerability Exploitability eXchange (VEX) - Status Justifications（2022 年 6 月）**
  VEX ドキュメントの最小要素における「脆弱性ステータス」のうち、「脆弱性の影響を受けない（NOT AFFECTED）」ステータスを正当化するための具体的な 5 つの主張を定義した文書。
  https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf
- **米国 CISA、NSA、ODNI : Securing Software Supply Chain Series - Recommended Practices for Developers（2022 年 9 月）**
  安全なソフトウェアサプライチェーンを確保するため、ソフトウェア開発者に対する推奨事項を整理した文書。本文書は、ソフトウェア開発者、ソフトウェアサプライヤー、ソフトウェア利用者の 3 つの役割ごとに焦点を当てた 3 部のガイダンスシリーズのうち、第 1 部に該当する。文書では、サードパーティコンポーネントを含むソフトウェアの SBOM の作成、脆弱性の評価等が推奨されている。
  https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
- **米国 CISA、NSA、ODNI : Securing Software Supply Chain Series -**

Recommended Practices for Suppliers（2022 年 10 月）
安全なソフトウェアサプライチェーンを確保するため、ソフトウェアサプライヤーに対する推奨事項を整理した文書。本文書は、ソフトウェア開発者、ソフトウェアサプライヤー、ソフトウェア利用者の 3 つの役割ごとに焦点を当てた 3 部のガイダンスシリーズのうち、第 2 部に該当する。文書では、サプライヤーは、開発者と利用者の間の仲介役として、ソフトウェアの保護や脆弱性に関する対応・通知等が推奨されている。
https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF

- **米国 CISA、NSA、ODNI : Securing Software Supply Chain Series - Recommended Practices for Customers（2022 年 11 月）**
  安全なソフトウェアサプライチェーンを確保するため、ソフトウェア利用者に対する推奨事項を整理した文書。本文書は、ソフトウェア開発者、ソフトウェアサプライヤー、利用者の 3 つの役割ごとに焦点を当てた 3 部のガイダンスシリーズのうち、第 3 部に該当する。文書では、サプライヤーへの SBOM の要求や SBOM を基にしたソフトウェアの脆弱性評価等が推奨されている。
  https://media.defense.gov/2022/Nov/17/2003116445/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_CUSTOMER.PDF

- **米国 CISA : Software Bill of Materials (SBOM) Sharing Lifecycle Report（2023 年 4 月）**
  SBOM の共有ライフサイクルに関するレポート。SBOM が作成者から利用者に共有されるまでに 3 つの基本フェーズがあるとし、各フェーズの概要とフェーズごとの洗練度合いが示されている。洗練度合いは、各フェーズを実施するために必要なコスト、リソース等の相対量を表しており、低・中・高のいずれかで定義される。また、SBOM の共有に関する現況を理解するため、関係組織に対して、組織が SBOM をどのように共有しているかのインタビュー結果が紹介されている。
  https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report

- **米国 CISA : Minimum Requirements for Vulnerability Exploitability eXchange (VEX)（2023 年 4 月）**
  VEX ドキュメントの最小要件を示した文書。本文書では、VEX ドキュメントを構成する項目と各項目に含まれる要素が示され、それぞれにおける必須項目・必須要件が定義されている。文書では、必須要件を VEX ドキュメントの最小要件と位置づけている。
  https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex

- **米国 CISA : Types of Software Bill of Materials (SBOM)（2023 年 4 月）**
  SBOM のタイプを定義した文書。本文書では、ソフトウェアライフサイクルの各フェーズで生成される可能性がある SBOM をタイプ分類し、各タイプの一般的な SBOM 生成方法、利点、制約が示されている。

https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom

- **オランダ NCSC：SBOM startersgids（2023 年 7 月）**
  組織における SBOM 導入を支援するガイド。本文書では、SBOM や VEX に関する基礎知識が概説されているほか、組織が SBOM を作成・管理・共有するためのプロセス、サプライヤーとの連携に向けた Tips が概説されている。加えて、代表的な脆弱性識別子に関する解説がなされているほか、組織内の脆弱性管理において SBOM を活用する方法についても示されている。
  https://www.ncsc.nl/documenten/publicaties/2023/juli/5/sbom-startersgids
- **ドイツ BSI：Technische Richtlinie TR-03183:Cyber-Resilienz-Anforderungen an Hersteller und Produkte（初版：2023 年 8 月、改定：2024 年 1 月）**
  SBOM の要件を示した技術ガイドライン。本ガイドラインでは、ソフトウェアベンダーを主な対象とし、SBOM のフォーマットに関する要件及び技術的な要件が記載されている。
  https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html
- **米国 CISA：Software Identification Ecosystem Option Analysis（2023 年 10 月）**
  ソフトウェア識別のエコシステムを実現するための主要な要件と具体的な実現方法を示したホワイトペーパー。本文書では、識別子の可用性と粒度に関する要件と各要件に対応する実現方法が示されている。
  https://www.cisa.gov/sites/default/files/2023-10/Software-Identification-Ecosystem-Option-Analysis-508c.pdf
- **米国 CISA、NSA、ODNI：Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption（2023 年 11 月）**
  ソフトウェアサプライチェーンのセキュリティ確保のための SBOM 利用に関するガイダンス。本ガイダンスでは、ソフトウェア利用者（例：サプライヤー、開発者、OSS・サードパーティ製のソフトウェアを取得する組織）による SBOM の利用に関する原則とベストプラクティスが示されている。
  https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF
- **米国 CISA：When to Issue VEX Information（2023 年 11 月）**
  VEX 情報を発行する組織・機能（Who）、VEX 情報が発行されるタイミング（When）の例示を整理した文書。文書では、ソフトウェアサプライチェーンにおける VEX の考慮事項についても示され

ている。
https://www.cisa.gov/sites/default/files/2023-11/When-to-Issue-a-VEX-508c.pdf

- **米国 CISA、NSA、ODNI : Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials（2023 年 12 月）**
  安全なソフトウェアサプライチェーンの確保に向けた OSS や SBOM の管理のための推奨プラクティスを示す文書。本文書では、OSS と SBOM の管理に関する 7 つのテーマに関して、推奨のプラクティスが示されている。
  https://media.defense.gov/2023/Dec/11/2003355557/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20MANAGING%20OPEN%20SOURCE%20SOFTWARE%20AND%20SOFTWARE%20BILL%20OF%20MATERIALS.PDF
- **米国 NSA : Recommendations for Software Bill of Materials (SBOM) Management（2024 年 1 月）**
  国家安全保障システム（NSS）のユーザーがサイバーセキュリティサプライチェーンリスク管理のニーズに適した SBOM 管理機能を組み込むことができるように、ベストプラクティスを強調し、推奨事項を提供する文書。ソフトウェアの供給者・利用者への推奨事項、NSS のための具体的な SBOM 管理指針、SBOM 管理ツールの機能に関する推奨事項が含まれる。
  https://media.defense.gov/2023/Dec/14/2003359097/-1/-1/0/CSI-SCRM-SBOM-MANAGEMENT.PDF
- **米国 CISA : SBOM Sharing Roles and Considerations（2024 年 3 月）**
  SBOM 共有ライフサイクルの 3 つの役割（SBOM 作成者、SBOM 配布者、SBOM 利用者）と、共有ライフサイクルの 3 つのフェーズ（Discovery、Access、Transport）に取り組む際に留意・注意すべき要素を記載した文書。
  https://www.cisa.gov/resources-tools/resources/sbom-sharing-roles-and-considerations
- **米国 CISA : SBOM Sharing Primer（2024 年 5 月）**
  SBOM をソフトウェアサプライチェーン上で共有する方法の例を複数提示した文書。それぞれの方法例は、3 つの洗練度合い（低・中・高）に分類され、企業はこの方法例を使用することで、自社の SBOM 共有プロセスがどの程度洗練しているかを判断できる。
  https://www.cisa.gov/resources-tools/resources/sbom-sharing-primer

10.3.2. SBOM に関するツール

本節では、SBOM の作成や運用・管理に資する SBOM ツールの一例を紹介する。有償の SBOM ツールだけでなく、無償の SBOM ツールも公開されており、ツールそれぞれに特徴がある。SBOM を導入する組織は、自組織の SBOM 導入の目的や SBOM 適用範囲を踏まえて、適切な SBOM ツールを選定することが望まれる。なお、本項に記載のツールはあくまで参考情報として手引作成時点での一例を挙げているにすぎず、特定のツールの利用を推奨するものではない。適切なツール選定のために、本項記載のツールに限定せず、市場に存在する様々なツールについて、4.2 に記載している観点を踏まえて評価・選定することが望まれる。

(1) 有償ツール

※ アルファベット順

No.	名称	開発者	特徴
1	Black Duck	Synopsys, Inc.	・ コードマッチング、コンテナ解析、バイナリ解析等の複数のスキャンアプローチにより、正確で効率的な解析が可能 ・ 脆弱性管理に関して、NVD 及び独自ソースの脆弱性情報を活用し、迅速な脆弱性検出が可能 ・ セキュリティ、ライセンス、コンプライアンス、運用等の観点でリスクを定量分析して管理 ・ 日本語の GUI を提供
2	Checkmarx SCA	Checkmarx Ltd.	・ Github における多くのリポジトリをホストすることで、使用されている OSS の自動的な追跡が可能 ・ 脆弱性管理に関して、ソースコード内に存在する脆弱な OSS のパッケージを検出し、対処方法を提示 ・ OSS のライセンスリスクを可視化し、効果的なライセンス管理が可能
3	Cybellum	Cybellum Technologies Ltd.	・ 脆弱性管理に関して、対象となるソフトウェア製品に存在する脆弱性を自動で検出し、検出した脆弱性の対応すべき優先順位や緩和策を提供 ・ ソフトウェア製品を継続的に監視し、ソフトウェアの更新プログラムや新しいバージョンのコンポーネントに存在する脆弱性を検出可能 ・ 複数の SBOM を取込み・一元管理することで、組織における SBOM の運用プロセスを統合可能

No.	名称	開発者	特徴
4	Finite State Platform	Finite State, Inc.	・ SBOM 及び脆弱性の統合管理プラットフォームを提供 ・ 様々な組込機器のアーキテクチャに対応し、バイナリやファームウェアからコンポーネントを可視化し SBOM を生成可能 ・ 150 種類以上の他社ツールの診断結果を取り込むことで脆弱性の一元管理が可能 ・ 攻撃発生状況など緊急度の高い脆弱性をトリアージし、対応優先度を判断可能 ・ SaaS、プライベートクラウド、オンプレミス等、複数の提供形態が存在
5	FOSSA	FOSSA, Inc.	・ 脆弱性検出と継続的なリスクモニタリングに加え、必要な解決方法の提示により、効果的な脆弱性管理を支援 ・ 高品質なポリシー機能と強力なスキャン、柔軟なレポートにより、コンプライアンス遵守及びライセンス管理を促進 ・ 開発環境との統合によりアジャイル・DevOps プロセスにおける SBOM 管理の自動化と効率化を実現 ・ SPDX 等の複数のレポート形式を選択可能なほか、複数の形式の SBOM をインポートして脆弱性管理が可能
6	FossID	FossID AB	・ コンポーネント、パッケージ、ライブラリだけでなく、OSS のスニペットレベルまで検出可能 ・ コンポーネントとバージョン情報に基づく解析ではなく、スニペットレベルの情報に基づいた解析によって、脆弱なソフトウェアを検出可能 ・ ライセンス、著作権、脆弱性等の情報を含む SPDX の形式で SBOM を生成し、管理が可能 ・ ライセンス管理に関して、強い/弱いコピーレフトや非商用のライセンス等の幅広い OSS のライセンス違反リスクを可視化
7	Insignary Clarity	Insignary, Inc.	・ バイナリファイルを解析して内包するコンポーネントを特定（ソースコードやリバースエンジニアリングは不要） ・ バイナリファイルのパターンを利用して解析するため、ビルド環境に依存せず解析可能 ・ クラウド及びオンプレミスのソフトウェアに対して適用可能 ・ クラウド型で提供されており、導入が容易

No.	名称	開発者	特徴
8	MEND SCA	WhiteSource Software, Inc.	・ クラウドサービス、デスクトップアプリ、組込ソフトウェア等で利用されている OSS のライブラリ・フレームワーク等を漏れなく検出可能 ・ 脆弱性管理に関して、常に最新状態に維持されている独自の脆弱性データベースを用いて脆弱性発生時に即時アラートを発行するほか、影響度や深刻度のスコアや解決方法の詳細情報も提供可能 ・ ライセンス管理に関して、IDE やパッケージマネージャー等の対象となるソフトウェアの開発環境へ本ツールを統合することにより、開発者が新しく OSS のコンポーネントを追加する都度、OSS のライセンス情報を自動で特定可能
9	MergeBase	MergeBase Software Inc.	・ SBOM を作成・管理する統合的なソフトウェアサプライチェーンセキュリティソリューション ・ コードやバイナリをスキャンし、脆弱性情報、ライセンス情報、年数情報、推移的依存性情報を含んだ SBOM を作成可能 ・ 脆弱性によるリスクの低減や改善方法の提案により、コード修正に要する労力を削減可能 ・ JVN と統合した脆弱性分析・管理が可能 ・ 国内パートナー企業と提携し、日本語版ドキュメントの提供や日本語による技術サポートを提供
10	Revenera SCA	Flexera Software LLC	・ ソースコード、バイナリ等のソフトウェア解析だけでなく、独自の OSS のナレッジデータベースやサードパーティの SBOM データを照合することで、正確な SBOM を作成可能 ・ NVD や独自の脆弱性データベース（Secunia Research）等の複数のソースを活用することで、効果的な脆弱性管理が可能
11	Snyk	Snyk, Ltd.	・ 既存の IDE、リポジトリ、ワークフローに組み込んで使用可能 ・ 高度なセキュリティインテリジェンスを使用し、対象となるソフトウェア開発中に脆弱性を監視 ・ 脆弱性管理に関して、脆弱性等に対する実用的な修正アドバイスを提供

No.	名称	開発者	特徴
12	Sonatype Lifecycle	Sonatype, Inc.	・ IDE やソースコード管理システム等の対象となるソフトウェアの開発環境へ本ツールを統合することで利用可能 ・ 脆弱性管理に関して、ソフトウェアやコンポーネントに含まれる脆弱性、脆弱性のリスクレベルを継続的に監視することで、迅速なアラートを発出可能
13	Veracode SCA	Veracode, Inc.	・ OSS のコンポーネント一覧として、CycloneDX 形式の SBOM を作成可能 ・ 脆弱性管理に関して、検出した脆弱性に対し、脆弱性の対処方法だけでなく、対処すべき優先順位を提示 ・ ライセンス管理に関して、OSS のライセンス違反リスクを検出し、ライセンスの遵守状況を管理することが可能
14	Yamory	株式会社アシュアード	・ 対象となる IT システムで利用されるソフトウェアの脆弱性を検知・管理可能 ・ 脆弱性管理に関して、オートトリアージ機能で脆弱性の優先度を自動で判断するほか、日次で脆弱性データベースを更新し、緊急性が高い脆弱性を早期に検知可能 ・ ライセンス管理に関して、OSS のライセンス違反リスクを可視化

(2) 無償ツール

※ アルファベット順

No.	名称	開発者	特徴
1	Augur	CHAOSS	・ ソフトウェアリポジトリに関するデータを収集し、データモデルに正規化 ・ OSS プロジェクトに関するデータを多くの情報源から収集
2	BOM Doctor	Sonatype, Inc.	・ Github 上のプロジェクトの URL やパッケージ URL を指定することで、SBOM を生成可能 ・ 生成された SBOM は、コンポーネントの依存関係を含めてツリー上に可視化（既存の CycloneDX 形式の SBOM をアップロードすることでも可視化可能） ・ 対象ソフトウェアに関して、脆弱でないコンポーネントを利用しているか、ライセンス違反していないか等を評価することで、スコアリングを実施

No.	名称	開発者	特徴
3	Checkov	Bridgecrew, Inc.	・ IaC 用の静的コード分析ツールでもあり、画像や OSS パッケージ用の SBOM ツールとしても活用可能 ・ スキャン結果は、CLI、CycloneDX、JSON、JUnit XML、CSV、SARIF、Markdown 形式で表示可能
4	Daggerboard	NewYork-Presbyterian Hospital	・ SBOM 及び関連する脆弱性を一目で確認・管理できるダッシュボードであり、SPDX 又は CycloneDX のファイルをインポートして脆弱性の検出が可能
5	Dependency-Track	OWASP Foundation	・ NVD、GitHub Advisories 等の複数のソースを活用し、サードパーティ及びオープンソースコンポーネントの既知の脆弱性を特定し、管理することが可能 ・ ソフトウェアコンポーネントのライセンス情報を特定可能 ・ API ファーストの設計により、他システムとの連携が容易
6	FOSSology	Linux Foundation	・ OSS の名称やバージョンの特定はできないものの、対象ソフトウェアに含まれるコンポーネントのライセンス及び著作権を検出し、管理することが可能 ・ Web UI を用いたインポートや解析が可能
7	in-toto	Linux Foundation	・ ソフトウェアがサプライチェーン内で配布中に改ざんされていないことを確認し、ソフトウェアサプライチェーンの整合性を保護するためのフレームワークを提供
8	mjcheck4	独立行政法人情報処理推進機構（IPA）	・ 独自の脆弱性データベースを活用することで、ソフトウェア製品に含まれる脆弱性の情報や脆弱性対策情報を提供 ・ SBOM のインポート・エクスポートが可能
9	OSS Review Toolkit (ORT)	Linux Foundation	・ ビルドシステムプラグインの適用等、既存のプロジェクトソースコードを変更することなしに SBOM の作成が可能 ・ カスタマイズ可能なポリシールールとライセンス分類に基づき、使用されているソフトウェアのライセンスを評価可能
10	OSV-Scanner	Google	・ CycloneDX 又は SPDX 形式で記述された SBOM のインポートが可能 ・ 独自の脆弱性データベースを活用することで、SBOM の各コンポーネントに含まれる脆弱性情報を提供

No.	名称	開発者	特徴
11	SBOM Tool	Microsoft Corporation	・ NPM、NuGet、PyPI 等の様々なパッケージ管理システムと統合して自動検出し、SPDX 形式の SBOM を作成することが可能 ・ Windows、Linux、macOS のプラットフォームで動作可能
12	ScanCode.io	nexB, Inc.	・ ソフトウェア構成分析（SCA）のプロセスをスクリプト化して自動化 ・ アプリケーションのコードベース内の OSS コンポーネントとそのライセンス情報を特定可能
13	Scancode Toolkit	nexB, Inc.	・ スタンドアロンのコマンドラインツールで、インストール、実行、CI/CD 処理パイプラインへの組み込みが容易 ・ スキャン結果を JSON、HTML、CSV、SPDX、独自の形式で保存可能 ・ ライセンス管理に関して、ユーザーによって拡張可能な独自の検出ルールを用いて、OSS コンポーネントのライセンス情報を特定し、管理することが可能
14	SW360	Eclipse Foundation	・ ソフトウェアコンポーネントにおけるセキュリティの脆弱性情報を特定し、管理することが可能 ・ ソフトウェアコンポーネントのライセンス情報を特定し、管理することが可能
15	SwiftBOM	CERT Coordination Center (CERT/CC)	・ 手動入力で SBOM 生成が可能 ・ 作成済み SBOM をインポートし、SBOM をツリー状に表示することが可能
16	Syft & Grype	Anchore Enterprise	・ Syft による SBOM 生成と、Grype による脆弱性検出機能をシームレスに連携可能 ・ CycloneDX、SPDX、Syft 独自のフォーマット等の SBOM フォーマット間で SBOM 情報を変換可能 ・ OS パッケージ、言語パッケージにおける主要な脆弱性を検知し、管理することが可能
17	Trivy	Aqua Security Software, Ltd.	・ 既知の脆弱性、IaC の構成ミス等の様々なセキュリティ問題を検知し、管理することが可能 ・ コンテナイメージ、ファイルシステム等の様々な対象をスキャン可能

10.3.3. SBOM のデータフォーマット

米国 NTIA の SBOM の「最小要素」には「自動化サポート」のカテゴリーが含まれ、SBOM の自動生成や可読性等の自動化をサポートすることが考慮されている。具体的なデータフォーマットとして、これまで国際的な議論がなされてきた SPDX、CycloneDX、Software Identification Tags（SWID タグ）の 3 つのフォーマットが位置づけられている。以降では、これら 3 つのフォーマットに加え、SPDX に基づき日本が開発したフォーマットである SPDX Lite の概要を示す。なお、フォーマットは継続的にアップデートされることが予想されるため、最新バージョンの把握に努めることが望ましい。また、SBOM のデータフォーマットは組織を越えて SBOM をやりとりするための一つの規格であり、データフォーマットの選定と SBOM に含めるべきデータフィールドの決定には、SBOM 利用者とサプライヤーとの間で合意の上で行われることが望まれる。

(1) SPDX

SPDX は、Linux Foundation の傘下のプロジェクトによって開発された。2021 年 9 月、ISO/IEC 5962:2021 の規格として、SBOM フォーマットの国際的な標準として認められている。SPDX の詳細な仕様は Web サイト上に公開[56]されており、プロジェクトにおいて検討・更新され続けている。2024 年 4 月には新たなバージョンである SPDX v3.0 が発表された。SPDX v3.0 では、より一般的な SBOM の生成と利用に関するユースケースに対応するため、セキュリティ・ライセンス・AI・データセット・ソフトウェア構築プロセスに重点が置かれている。

以降では、SPDX の v2.3.0 の概要として、フォーマットの構成、フォーマットの使用例・使用目的、フォーマットの特徴を示す。

1) フォーマットの構成

SPDX フォーマットにおける SBOM では、SPDX Specification にしたがって作成されたコンポーネントやライセンス、コピーライト等の情報が記載され、Tag:Value(txt)形式、RDF 形式[57]、xls 形式、json 形式[58]、YAML 形式[59]、xml 形式[60]がサポートされている。SBOM ドキュメントに含める内容として、セクションと各セクションに分類される項目が規定されている。各セクションの概要を以下に示す。なお、「SBOM ドキュメントの情報（Creation Information）」のセクションのみが必須と定義され、必須で

---

[56] https://spdx.github.io/spdx-spec/v2.3/

[57] RDF 形式のファイルを解析する方法として、例えば、ファイルに記述されたデータの検索や操作を行うための SPARQL 言語を活用することが知られている。

[58] json 形式のファイルを解析する方法として、例えば、ファイルから必要情報を取得するための jq コマンドを活用する方法が知られている。

[59] Visual Studio Code や IntelliJ IDEA 等の YAML 形式のファイルに対応するツールを使用することで、ファイルの閲覧や解析が容易となる。

[60] xml 形式のファイルを解析する方法として、例えば、ファイルから必要情報を取得するための xmllint コマンドを活用する方法が知られている。

はないほかのセクションについては、SBOM ドキュメント作成者が SBOM に含めるべきと判断する場合に使用する。また、各セクションに規定された項目のうち、該当セクションを使用する場合に必須で含めるべき項目も決められている。

- **SBOM ドキュメントの情報（Creation Information）【必須セクション】：**
  サプライヤーが SBOM ドキュメントを提供し、利用者が SBOM ドキュメントを活用するために必要な情報（SPDX バージョン、SBOM データライセンス、作成者等）を提示するセクション。本セクションは、SPDX による SBOM ドキュメントに必ず含める必要がある。
- **パッケージ情報（Package Information）：**
  SBOM 内にて、製品、コンテナ、コンポーネント等をグループ化するために必要な情報を提示するセクション。
- **ファイル情報（File Information）：**
  製品、コンテナ、コンポーネント等のファイルに関する情報（名称、チェックサム、ライセンス、著作権等）を提示するセクション。
- **スニペット情報（Snippet Information）：**
  あるファイルがほかのリソースから生成されている場合に使用するセクション。本セクションは、ファイルの一部が他のファイルからコピーされたことを示す際に有効である。
- **その他ライセンス情報（Other Licensing Information）：**
  SPDX では、ファイル情報のライセンスを提示するための SPDX ライセンス一覧と呼ばれるライセンス一覧が定義されている。「パッケージ情報」、「ファイル情報」、「スニペット情報」のセクションでは、説明対象となるパッケージ、ファイル、スニペットのライセンス情報として、SPDX ライセンス一覧から選択して使用する。ただし、SPDX ライセンス一覧は、パッケージ、ファイル、スニペットに関するすべてのライセンスを網羅していないため、本セクションで、SPDX ライセンス一覧以外のライセンス情報（プロプライエタリソフトウェアによる制限等）を提示することが可能である。
- **リレーションシップ（Relationships）：**
  SBOM 内における製品、コンテナ、コンポーネント等のファイルやパッケージの関係を提示するセクション。
- **注釈（Annotations）：**
  SBOM をレビューし、そのレビュー結果から得た情報を他者へ共有するために使用されるセクション。加えて、SBOM ドキュメントの作成者が、前述した他セクションや項目に当てはまらない情報を SBOM 内に保管したい場合でも本セクションを使用することが可能である。

2) 使用例・使用目的

SPDX の使用例・使用目的として、以下が想定される。

- システムの構成要素と構成要素間の関係性を記述する

- ソフトウェアコンポーネントの知的財産（ライセンス、著作権）を管理する
- ソフトウェアサプライチェーンのリスクアセスメントとコンポーネントを検証する
- ソフトウェアコンポーネント、コンテナコンテンツ等のインベントリーを作成する
- ソースファイルやソーススニペットに遡って実行ファイルを追跡する
- ファイルに埋め込まれたコードの出所を特定する
- ソフトウェアを一意に特定するためのフォーマットである CPE、SWHID（SoftWare Heritage persistent IDentifiers）、パッケージ URL 等を特定のパッケージに関連付け、追加のセキュリティ分析を容易にする

3) データフォーマットの特徴

SPDX の特徴として、以下が挙げられる。

- SBOM の作成対象となるソフトウェアとして、スニペットやファイルに留まらず、パッケージ、コンテナ、OS ディストリビューションまで拡張可能
- SBOM ドキュメントとして作成された成果物は、提供されたハッシュ値を使用することで SBOM データの改ざん有無を検証することが可能
- 知的財産とライセンス情報のための豊富なリスト（SPDX ライセンス）を持つ
- 他のパッケージ参照システムやセキュリティシステムと連携することが可能
- 複雑なシステムに関連するドキュメントを論理的に分割し、SBOM ドキュメントの各セクションや項目で管理することが可能

(2) SPDX Lite

SPDX Lite は、Linux Foundation の傘下のプロジェクトである OpenChain Project における日本企業を中心として活動する、OpenChain Japan Work Group (WG) のライセンス情報サブグループによって開発された日本発のフォーマットである。SPDX Lite は、SPDX に関する ISO/IEC 5962:2021 規格の一部に含まれ、SPDX に内包される位置づけとして定義されている。SPDX Lite の詳細な仕様は、SPDX の v2.3.0 の仕様の一部として、Web サイト上に公開[61]されている。以降では、SPDX Lite の概要として、フォーマットの構成と具体的な項目、フォーマットの使用例・使用目的、フォーマットの特徴を示す。

[61] https://spdx.github.io/spdx-spec/v2.3/SPDX-Lite/

1) フォーマットの構成と具体的な項目

SPDX Lite フォーマットにおける SBOM では、コンポーネントやライセンス、コピーライト等の情報が記載され、Tag-Value(txt)形式、RDF 形式、xls 形式、json 形式、YAML 形式、xml 形式がサポートされている。SBOM ドキュメントに含める内容として、前述した、SPDX における「SBOM ドキュメントの情報」と「パッケージ情報」のセクションに分類される必須項目とその他の基本情報で構成される。SPDX Lite に求められる項目は以下に示すとおりである。

表 10-2 SPDX Lite の項目と SPDX との対応関係

SPDX におけるセクション名	SPDX Lite の項目名
SBOM ドキュメントの情報（Creation Information）	SPDX バージョン（SPDX Version）
	SBOM のデータライセンス（Data License）
	ドキュメント ID（SPDX Identifier）
	ドキュメント名（Document Name）
	ドキュメント名前空間（SPDX Document Namespace）
	ドキュメント作成者・作成ツール（Creator）
	ドキュメント作成日（Created）
パッケージ情報（Package Information）	パッケージ名称（Package Name）
	パッケージ ID（Package SPDX Identifier）
	パッケージバージョン（Package Version）
	パッケージファイル名（Package File Name）
	パッケージサプライヤー名（Package Supplier）
	パッケージのダウンロード場所（Package Download Location）
	パッケージファイル解析情報（Files Analyzed）
	パッケージのホームページ（Package Home Page）
	パッケージへ締結されたライセンス（Concluded License）
	パッケージ作成者が宣言する適用ライセンス（Declared License）
	ライセンスに関するコメント（Comments on License）
	パッケージの著作権（Copyright Text）
	パッケージに関するコメント（Package Comment）
	パッケージに関する外部参照情報（External Reference field）
その他ライセンス情報（Other Licensing Information）	ライセンス ID（License Identifier）
	ライセンス情報（Extracted Text）
	ライセンス名（License Name）
	ライセンスに関するコメント（License Comment）

2) 使用例・使用目的

SPDX Lite の使用例・使用目的として、以下が想定される。

- 「SBOM ドキュメントの情報」と「パッケージ情報」の SPDX セクションに分類される必須項目のみを手動で管理する
- SPDX が定義するプロパティ全体をカバーする SBOM ではなく、自動車業界や家電業界等で最低限要求された項目に対応し、運用性を重視した SBOM を作成する

3) データフォーマットの特徴

SPDX Lite の特徴として、以下が挙げられる。

- SPDX と比べて必要最低限の項目のみが含まれているため、運用性を重視した SBOM 管理が可能
- SPDX の「SBOM ドキュメントの情報」と「パッケージ情報」のセクションに分類される必須項目を含んでいるため、SPDX に対応した SBOM ツールと親和性が高い
- SPDX Lite 形式の SBOM 作成に当たって、専用のツールは必要なく、手動で SBOM ドキュメントを作成することが可能

(3) CycloneDX

CycloneDX は、完全自動化可能で、セキュリティに特化した SBOM フォーマットの標準を開発することを目標として、OWASP コミュニティのプロジェクトによって開発された。CycloneDX の詳細な仕様は、WEB サイト上に公開[62]されており、OWASP コミュニティのコアワーキンググループで管理、更新され続けている。2024 年 4 月には、新たなバージョンである CycloneDX 1.6 が発表された。以降では、CycloneDX の v1.5 の概要として、フォーマットの構成、フォーマットの使用例・使用目的、フォーマットの特徴を示す。

1) フォーマットの構成

CycloneDX フォーマットによる SBOM では、コンポーネントやライセンス、コピーライト等の情報が記載され、json 形式、xml 形式、Protocol Buffers (protobuf)形式がサポートされている。SBOM ドキュメントに含める内容として、オブジェクトモデルと各オブジェクトモデルに分類される項目が規定されている。各オブジェクトモデルの概要を以下に示す。また、各オブジェクトモデルに規定された項目のうち、該当モデルを使用する場合に必須で含めるべき項目も決められている。なお、オブジェクトモデルには分類されないものの、SBOM ドキュメントが CycloneDX フォーマットであること、CycloneDX のバージョンに関する項目を含めることが、必須とされている。

[62] https://cyclonedx.org/docs/1.5/json/

- **SBOM のメタデータ（SBOM Metadata）：**
  サプライヤー、開発者、SBOM ドキュメントが対象とするソフトウェアの範囲、SBOM ドキュメントを作成するために使用したツール等の情報を提示するオブジェクトモデル。

- **コンポーネント（Components）：**
  ファーストパーティ及びサードパーティのソフトウェアコンポーネントのインベントリーを提示するオブジェクトモデル。本オブジェクトモデルには、ソフトウェアコンポーネントの種類、ID、ライセンス、著作権、暗号的ハッシュ関数、系譜、来歴、加えられた変更内容等の情報を含めることが可能である。また、本オブジェクトモデルでは、コンポーネントの組合せを表現することができ、組合せられたコンポーネントは、一つのコンポーネントとして各種情報を保有することが可能である。さらに、コンポーネントや組合せられたコンポーネントにデジタル署名を適用することが可能である。

- **外部サービス（Services）：**
  SBOM ドキュメントが対象とするソフトウェアが呼び出す可能性のある外部 API の情報を提示するオブジェクトモデル。本オブジェクトモデルには、外部 API のエンドポイント URI、認証要件、外部 API との信頼境界線、サービス間とのデータの流れ・分類等の情報を含めることが可能である。さらに、サービスにデジタル署名を適用することが可能である。

- **依存関係（Dependencies）：**
  コンポーネントと他のコンポーネント間の依存関係を提示するオブジェクトモデル。コンポーネント同士だけでなく、サービスに依存するコンポーネントやサービスに依存するサービスも表現することが可能である。また、依存関係は、推移的依存関係を表現することが可能である。

- **構成要素の完全性（Compositions）：**
  SBOM 内における各構成要素（コンポーネント、サービス、依存関係を含む）と構成要素の完全性を提示するオブジェクトモデル。各構成要素は、「完全である」、「不完全である」、「不完全なファーストパーティのみである」、「不完全なサードパーティのみである」、「不明である」のように表現することが可能である。本オブジェクトモデルによって、作成された SBOM がどの程度完全であるか、SBOM 内に完全性が不明な構成要素があるかを理解することが可能である。

- **脆弱性（Vulnerabilities）：**
  SBOM に含まれるサードパーティソフトウェアや OSS に存在する既知の脆弱性とその脆弱性の悪用可能性を提示するオブジェクトモデル。また、コンポーネントやサービスに影響を与える未知の脆弱性も提示することを可能とし、VEX 等のセキュリティアドバイザリーとして使用することが可能である。

- **配合（Formulation）：**
  SBOM に含まれるコンポーネントやサービスがどのように製造又は展開されたかを提示するオブジェクトモデル。本オブジェクトモデルでは、ソフトウェアの製造プロセスで発生したアクションが、ワークフロー・タスク・手順等で記述される。

- **注釈（Annotations）：**

コンポーネント、サービス、脆弱性、SBOM ドキュメント等に関して、SBOM の利用者や組織関係者による注釈を提示するオブジェクトモデル。本オブジェクトモデルには、様々な利害関係者からの意見やコメントが記述される可能性がある。

- **拡張機能（Extensions）：**
  CycloneDX における新しい機能の試行、特殊なユースケースや将来のユースケースのサポートを可能にするオブジェクトモデル。CycloneDX プロジェクトでは、専門的や業界固有のユースケースを対象とする拡張機能に関するコミュニティへの参加や開発を推奨している。

2) 使用例・使用目的

CycloneDX の使用例・使用目的として、以下が想定される

- システムの構成要素と構成要素間の関係性を記述する
- ソフトウェアコンポーネントの知的財産（ライセンス、著作権）を管理する
- ソフトウェアサプライチェーンのリスクアセスメントとコンポーネントを検証する
- ソフトウェアコンポーネント、コンテナコンテンツ等のインベントリーを作成する
- ソースファイルやソーススニペットに遡って実行ファイルを追跡する
- ファイルに埋め込まれたコードの出所を特定する
- ソフトウェアを一意に特定するためのフォーマットである CPE、SWID、パッケージ URL 等を特定のパッケージに関連付け、追加のセキュリティ分析を容易にする
- 署名されたコンポーネントや組合せられたコンポーネントと SBOM の整合性を検証する
- ソフトウェアのビルド時における作成・配布に便利なフォーマット、M2M（マシンツーマシン）でのバイナリフォーマットとして利用する
- ソフトウェアの製造方法や手順を追跡する

3) データフォーマットの特徴

CycloneDX の特徴として、以下が挙げられる。

- セキュリティ管理を念頭に置いた SBOM フォーマットであり、既知の脆弱性に関する情報や、その脆弱性の悪用可能性に関する情報を記載できる
- アプリケーション、コンポーネント、サービス、ファームウェア、デバイス等の様々な種類のソフトウェアに対応したセキュリティに関する SBOM フォーマットであり、幅広い業界で使用され商用利用に適している
- CycloneDX は、体系立てられたオブジェクトモデルで構成されるフォーマットであるため、学習と

導入が容易

- 多くの開発エコシステムと統合することによって自動化を実現
- 仕様の拡張が可能なため、組織や業界特有の要件に応じた新しい機能の迅速な試行が可能
- ソフトウェアの製造方法や手順の詳細を追跡することで、ソフトウェアのセキュリティに係る理解が容易となり、ソフトウェアの安全性や潜在的なリスクの評価ができる

(4) SWID タグ

SWID タグは、組織が管理対象とするデバイスにインストールされたソフトウェアを追跡することを目標として開発された。2012 年に ISO で定義され、2015 年に ISO/IEC 19770-2:2015 として更新された。SWID タグでは、ソフトウェアライフサイクルに沿ったソフトウェアのインストールプロセスの一貫として、デバイスにソフトウェアがインストールされるとタグと呼ばれるインストールされたソフトウェアの情報がデバイスに付与され、アンインストールされるとタグが削除される。以降では、SWID タグの概要として、フォーマットの構成、フォーマットの使用例・使用目的、フォーマットの特徴を示す。

1) フォーマットの構成

SWID タグフォーマットによる SBOM では、SWID タグにしたがって作成されたデバイスにインストールされたソフトウェアやソフトウェアに適用したパッチ等の情報が記載され、xml 形式がサポートされている。SWID タグは、対象とするデバイスのライフサイクルを把握するために、デバイスにインストールされたソフトウェアの情報を示すタグが規定されている。各タグの概要を以下に示す。各タグでは、タグの作成者、デバイスにインストールされるソフトウェア、他のソフトウェアへのリンクによる依存関係等の情報を提示することができ、対象とするデバイスの SBOM として使用することが可能である。

- **プライマリータグ（Primary Tag）：**
  対象とするデバイスにインストールされたソフトウェアを識別、提示するタグ。
- **パッチタグ（Patch Tag）：**
  対象とするデバイスにインストールされたソフトウェアに対して、アップデート等で適用したパッチを識別、提示するタグ。
- **コーパスタグ（Corpus Tag）：**
  対象とするデバイスにインストールするソフトウェアを特定し、説明するタグ。本タグは、ソフトウェアのインストールパッケージ、インストーラー、ソフトウェアアップデート、パッチ等のソフトウェアのメタデータを表現するために使用される。
- **サプリメントタグ（Supplemental Tag）：**
  上記のタグに関する情報に、追加的な情報を付与するためのタグ。デバイスの利用者やソフトウェア管理ツールが、任意の情報を追加するために本タグが使用される。

2) 使用例・使用目的

SWID タグの使用例・使用目的として、以下が想定される。

- 組織で管理しているデバイスにインストールされたソフトウェアをコンポーネントとして、SBOM を作成する
- デバイスにインストールされたソフトウェアを継続的に追跡する
- エンドポイントにおける脆弱なソフトウェアを特定する
- デバイスにインストールされたソフトウェアが、適切にパッチを適用しているかを確認する
- 不正なソフトウェアや破損したソフトウェアのインストールを防止する
- 破損したソフトウェアの実行を防止する
- 管理対象のデバイスに関するユーザーの権利やアクセス権等を管理する

3) データフォーマットの特徴

SWID タグの特徴として、以下が挙げられる。

- ソフトウェアライフサイクルに合わせて各タグの情報を更新するため、ビルド時に作成されるソフトウェア ID の情報を正確にタグへ付与して提供することが可能
- ソフトウェアのインストール時に、サプライヤーと利用者の間で交換可能なソフトウェア情報を標準化
- 関連するパッチやアップデート、構成設定、セキュリティポリシー、脆弱性や脅威の勧告等、ソフトウェアに関連する情報の関連付けが可能